

RIGHT TO PRIVACY VIS-À-VIS NATIONAL SECURITY - HARMONISING
THE CONFLICTING INTERESTS



Dissertation submitted to National Law University, Assam

In partial fulfillment for the award of the degree of

MASTER OF LAWS

Supervised By-

Dr. Lohit D. Naikar

Visiting Professor of Law

Submitted by-

Ms Smriti Katiyar

SF0219028

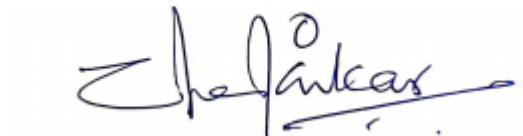
2019-2020, Semester II

National Law University, Assam

August 2020

SUPERVISOR CERTIFICATE

It is to certify that Ms. Smriti Katiyar is pursuing a Master of Laws (LL.M.) from National Law University, Assam, and has completed her dissertation titled “Right to Privacy Vis-À-Vis National Security - Harmonising the Conflicting Interests” under my supervision. The research work is found to be original and suitable for submission.

A handwritten signature in blue ink, appearing to read 'Lohit D. Naikar', is centered on a light gray grid background.

Dr. Lohit D. Naikar

Visiting Professor of Law

Date: 22.08.2020

DECLARATION

It is to certify that Ms. Smriti Katiyar is pursuing Master of Laws (LL.M.) from National Law University, Assam, and has completed her dissertation titled “Right To Privacy Vis-À-Vis National Security -Harmonizing the Conflicting Interests under my supervision.” The research work is found to be original and suitable for submission.



Date: 22.08.2020

Ms Smriti Katiyar

SF0219028

Table of Contents

CERTIFICATE.....	i
DECLARATION.....	ii
PREFACE.....	viii
ACKNOWLEDGMENT.....	xii
TABLE OF CASES	xiii
TABLE OF STATUTES.....	xvi
TABLE OF ABBREVIATIONS	xvii
CHAPTER 1.....	1
INTRODUCTION.....	1
CHAPTER 2.....	8
RESEARCH METHODOLOGY.....	8
2.1. Research Background.....	8
2.3. Aim.....	10
2.4. Objectives.....	12
2.5. Scope.....	13
2.6. Literature Review.....	13
2.7. Research Question.....	20
2.8. Research Method Applied to Test Hypothesis.....	21
2.9. Research Design.....	23
2.9.1. Approach.....	23
2.9.2. Tools of Data Collection.....	23
CHAPTER 3.....	24
3.1. Philosophy of Privacy.....	24
3.2. Concept of Privacy.....	28

3.3. Need of Privacy.....	31
3.4. Privacy as a Trade-Off.....	34
3.5. State Power.....	40
3.5.1. Genesis.....	40
3.6. Constitution and Definition of Constitution.....	41
3.7. Importance of ROL in Maintaining Constitutionalism.....	42
3.8. Limited Government: Origin and Scope.....	43
CHAPTER 4.....	46
LEGAL FRAMEWORK.....	46
4.1. Right to Privacy.....	46
4.2. International Perspective of Primary Rights.....	48
4.2.1. Viewpoints on Privacy.....	50
4.2.2. The USA and the Right to Privacy.....	51
4.3. Privacy Laws in Other Countries.....	57
4.3.1. European Union.....	57
i. Expansion of Primary Laws.....	57
4.3.2. Australia.....	58
4.3.3. Sweden.....	58
4.3.4. Germany.....	59
4.3.5. South Africa.....	59
4.3.6. Canada.....	60
4.3.7. Japan.....	60
4.4. Right to Privacy in India.....	62
4.4.1. Historical Development in India.....	62
i. Right to Privacy in India before Independence.....	63
ii. Constitution of India Bill, 1895.....	63

iii. The Common Wealth of India Bill, 1925.....	64
iv. The Nehru (Swaraj) Report, 1928.....	64
v. Constituent Assembly (CA) Debates on the Right to Privacy.....	64
4.5. Data Protection Laws in India.....	66
4.5.1. Information Technology Act, 2000.....	67
4.5.2. Information Technology Rules, 2011.....	69
4.5.3. Intellectual Property Rights.....	71
4.5.4. Indian Penal Code.....	71
4.6. Industry Initiative.....	71
4.7. Role of Courts: Case Analysis.....	74
4.8. Analysis of 2017 Judgement of Justice K.S.Puttaswamy and ANR.V Union of India and DRS Number.....	82
CHAPTER 5.....	88
NATIONAL SECURITY LEGISLATIONS AND THEIR EFFECT ON PRIVACY.....	88
5.1. The Unlawful Activities (Prevention) Act, 1967.....	88
5.1.1. A Brief History of UAPA.....	88
5.1.2. Reasons for Legislating the Act.....	89
5.1.3. Why was the UAPA unique.....	90
5.2. Similar Legislation as the UAPA.....	92
5.3. Further Amendments to the UAPA, making it as Draconian as it Stands.....	95
5.3.1. The Final Immoral Amendment in 2019.....	96
5.4. Privacy Concerns over the said Acts.....	99
5.5. Peroration.....	103
5.6. UAPA as a law being misused.....	104
CHAPTER 6.....	107

INTERPRETATION AND ANALYSIS.....	107
6.1. Major Issues and Concerns: Impact of 2017 Judgement.....	107
6.1.1 Data Protection and Aadhar-The Biometric Authentication System....	108
6.1.2. The Linkage Problem.....	111
6.1.3. Data Security and Infringement.....	113
6.1.4. Comparison to Social Security Number.....	114
6.2. Negative And Positive Aspect.....	115
6.3. Need of Primary Laws in India.....	117
6.3.1. Necessity of Legislation of Right to Data Privacy.....	118
6.3.2. Necessity of Legislation of Right to Data Privacy (2017).....	120
6.3.3. Precedents and History.....	120
6.3.4. Objectives of the Proposed Bill.....	121
i. Establishing the Right to Privacy.....	121
ii. Standard Operating Procedure For Data Collection Transfer And Storage.....	122
iii. National Security Implications.....	123
iv Safeguards & Constitutional Authority.....	123
6.4. Philosophy and Instances of Mass Surveillance.....	124
6.5. Indian Privacy Code, 2018.....	129
6.6. Brief Analysis on How National Security Agencies Pierce the Right to Privacy of the Citizens under the Excuse of National Security....	133
6.7. Mobile Application Ban (2020).....	139
6.7.1. Violation of Fundamental Rights.....	139
6.7.2. Whether the Application Ban is Justifiable.....	141
6.7.3. Invoking the National Security Exception under WTO Framework.....	143

6.8. Peroration.....	143
CONCLUSION.....	144
BIBLIOGRAPHY.....	xx

PREFACE

If one were to visit the Cellular Jail in Andaman & Nicobar Islands, they would unwittingly admire the peculiar manner in which the building has been designed, wherein the six blocks, housing one hundred and sixteen prison cells each have been built to resemble the spokes of a wheel emanating from a high watchtower in the center, which was used to station the prison security. However, very few would realize that the building was designed in this unique manner not to serve any aesthetic purpose, but to deliberately enable the prison guards to constantly observe the behaviour of the prison inmates in their solitary cells, without even being seen by them. Over time, it would allow those in power, such as the State acting through its prison guards in the present example, to use the knowledge gathered by observing its subjects, such as the political prisoners in the jail, to discriminate, blackmail, stifle and oppress them if they were to ever pose a threat to their power whilst at the same time maintaining a stronghold over their power by deciding what is and what is not socially acceptable behaviour. This form of constant monitoring by an authority in power would ultimately have a chilling effect wherein the subjects of power would be coerced to unquestioningly abide by any law imposed by the authority.

Unfortunately, this method of surveillance is still employed in present times by the modern state and private associations to gather information about the location, activities, associations, preferences, and behaviour of individuals, whether incarcerated or innocent, through various technologies such as CCTVs, whole-body imaging scanners, RFID enabled documents, biometrics as well as through gag orders and laws that allow roving wiretaps or that make it mandatory to provide personal information at the time of enrolment or employment or that allow intercepting personal communication or disclosure of sensitive personal information in the name of safeguarding national security and public interest, thereby enabling such entities to constantly intrude into the personal lives of individuals and gather such information as may be useful to

serve their vested interest. In such a scenario, should we individuals surrender ourselves at the altar of this invisible power that aims to control us so that it can further its own end goals? Should we sacrifice our freedoms to attain greater security and social good? Or do we have a right to be left alone? Essentially, do we have a right to privacy, whether absolute or qualified?

However, before we can claim that every individual has a right to privacy, it becomes necessary to establish what we mean by the term privacy. Unfortunately, the concept of privacy is in disarray because there is no clear consensus on what constitutes privacy – whether and to what extent it encompasses space, location, communication, data, behaviour, association, action, thoughts, and feelings of an individual. The lack of clarity in defining privacy makes the task of defining the acts that constitute a violation of the right to privacy all the more difficult. Thus, it becomes easy to infringe the right to privacy of individuals simply because the grounds on the opposite side such as security, public interest, executive, and judicial necessity have been articulated better as concepts *qua* the concept of privacy. Consequently, issues of privacy violations are often deflated not only by Courts and policymakers but also by individuals themselves who routinely give out personal information without thinking of its larger repercussions. Therefore, it is necessary to establish the various facets of privacy as an independent concept and thereafter safeguard the right to privacy of every individual, because not only is privacy an essential bulwark of a democratic society but also important for the autonomy, freedom, creativity and psychological well-being of an individual.

In the backdrop of this growing discussion about privacy in the last few decades, several multinational laws, guidelines, and directives have been formulated to protect the right to privacy. For instance, The United Nations Universal Declaration of Human Rights, 1948 stipulates that “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation.” The International Covenant on Civil and Political Rights states that “No one shall be subjected to arbitrary or unlawful interference with his privacy, family, or correspondence, or to unlawful attacks on his honor and reputation Similarly,

The European Convention of Human Rights, 1950 provides that “everyone has the right to respect for his private and family life, his home and his correspondence.” In pursuance of these international obligations, several nations across the globe have made an effort to protect the right to privacy. For instance, even though the constitution of the USA nowhere explicitly mentions the term privacy, the Courts have interpreted its provisions to include the right to privacy implicitly, thereby safeguarding the decisions that people make about their sexual conduct, birth control, and health from any arbitrary and unwarranted interferences by the State. The UK, on the other hand, has enacted the Data Protection Act, 1998 which governs how the personal information of individuals may be used and prevented from breaches by the State and third parties.

Moreover, the Supreme Court of India, in a recent landmark judgment, has explicitly granted the right to privacy as an independent right to all individuals. However, while on one hand, the apex Court has granted all individuals a right to privacy, the legislature, on the other hand, has been tardy in amending the existing policies and laws which infringe the right such as the AADHAR Act, policy on collection and storage of biometric data, policy on maintaining the privacy of medical records and Section 377 which criminalizes homosexual acts as well as in enacting additional laws to strengthen protection to the right in areas where there is a lacuna such as comprehensive laws to protect data, regulating data trading and safeguarding financial privacy. Therefore, while the Courts in the UK have not only formulated but also implemented that “every Englishman’s home is his castle” where the individual has the “right to be let alone”, it will be interesting to view how the right to privacy, which has been recently guaranteed to the individuals in India, is interpreted, developed and upheld soon.

In the debate of privacy versus national security, one must not forget that if privacy is dear to the individual, so is the security of the state, the individual lives in. How far is one willing to go and waive off his right to privacy in order to help the state for collection of data and using the information for security measures? Upto what extent should there be Intervention by state and should they be given unchecked, unsolicited and unfettered power to obtain the

data through surveillance? Various bills have been passed and measures have been taken to harmonize the conflicting interests of both.

ACKNOWLEDGEMENT

First, I would like to express my sincere gratitude to Prof. Lohit. D. Naikar, Visiting Professor of Law, National Law University, Assam for his consent, support, and encouragement as well as his invaluable suggestions and inputs throughout this research. His guidance and direction have been significant in the completion of this seminar paper for which I am thankful to him

Secondly, I would like to especially thank Prof. (Dr.) J.S. Patil, the Vice-Chancellor of National Law University, Assam for sharing with us his vast knowledge in the field of legal research through his vigorous lecture. His teachings on research methodology have greatly helped me in approach to his research.

Thirdly, I would like to thank my fellow batchmates and beloved junior who have helped me in different stages in the preparation of this study

Finally, I am grateful to my parents and friends for their unending support and for providing all the necessities in preparing this paper.

Thanking You

Yours Sincerely

Smriti Katiyar LL.M. 2nd Semester

A handwritten signature in black ink, reading "Smriti Katiyar". The signature is written in a cursive style with a horizontal line underlining the name.

TABLE OF CASES

1. *A. K. Gopalan vs. State of Madras*
2. *Arup Bhuyan v. State of Assam*
3. *Board of Trustees of the Port of Bombay v. Dilip Kumar Raghavendranath Nadkarni*
4. *Bowers vs. Hardwick*
5. *Carey vs. Population Services International*
6. *Cleveland Board of Education vs. LaFleur*
7. *Cruzan vs. Director, Missouri Department of Health*
8. *District registrar and collector, Hyderabad and another v. Canara Bank and another*
9. *Douglas v Hello Ltd*
10. *Eisenstadt vs. Baird*
11. *Eisenstadt vs. Baird and Roe vs. Wade*
12. *Gobind vs. State of Madhya Pradesh*
13. *Govind vs. State of Madhya Pradesh*
14. *Griswold vs. Connecticut*
15. *Hukam Chand Shyam Lal vs. Union of India and Ors.*
16. *Justice K.S. Puttaswamy and Anr. Vs. Union of India and Ors*
17. *Kaleidoscope (India)(P) Ltd. vs. Phoolan Devi*
18. *Kartar Singh v. State of Punjab*

19. *Kesavananda bharati v. statate of kerela*
20. *Kharak Singh vs. State of Uttar Pradesh*
21. *Lawrence vs. Texas*
22. *M. Malkani vs. State of Maharashtra*
23. *M.P. Sharma vs. Satish Chandra*
24. *Maneka Gandhi vs. Union of India*
25. *Moore vs. City of East Cleveland*
26. *Mr 'X' vs. Hospital 'Y'*
27. *People's Union for Civil Liberties (PUCL) v Union of India*
28. *Petronet LNG LTD v, Indian Petro Group and Another*
29. *Pierce vs. Society of Sisters*
30. *Poe vs. Ullman*
31. *R. C. Cooper vs. Union of India*
32. *R. Rajagopal vs. State of Tamil Nadu*
33. *R.Rajagopal v. Union of India*
34. *Radhakrishan vs. State of U.P*
35. *Roe vs. Wade*
36. *Selvi and others v. State of Karnataka and others*
37. *ShayaraBano&Ors. v. Union of India &Ors*
38. *Sri Indra Das v. State of Assam*
39. *State of Maharashtra vs. Natwarlal Damodardas Soni*
40. *State of UP vs. Kaushaliya*
41. *Troxel vs. Granville*

42. *Union of India v. Students Islamic Movement of India*
43. *Unique Identification Authority of India & anr v. Central Bureau of Investigation*
44. *Veena Seth v. State of Bihar*

TABLE OF STATUTES

1860 - Indian Penal Code

1885 - Indian Telegraph Act

1949 - Constitution of India

1980 - National Security Act

1987 - Terrorist and Disruptive Activities (Prevention) Act

2000 - Information Technology Act

2002 - The Prevention of Terrorism Act

2005 – Right To Information Act

2016 - The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act

2019 - Unlawful Activities (Prevention) Amendment Act

ABBREVIATION

AI	Amnesty International
AIR	All India Reporter
ALRC	Australian Law Reform Commission
AP	Andhra Pradesh
APDR	Association for the Protection of Democratic Rights
APPI	Act on the Protection of Personal Information
Art.	Article
Bom.	Bombay
Cal	Calcutta
CBI	Central Bureau of Investigation
CJI	Chief Justice of India
CLAHRO	Civil Liberties and Human Rights Organization
CRC.	Convention on Rights of Child
Cri LJ	Criminal Law Journal
CrLR	Criminal Law Review
CrPC	Code of Criminal Procedure
Dy SP	Deputy Superintendent of Police
ECHR	European Commission on Human Rights
Etc.	Et cetera
EU	European Union
F.I.R	First Information Report
FR	Fundamental Rights
Govt.	Government
HC	High Court
HRW	Human Rights Watch
IB	Intelligence Bureau
ICCPR	International Covenant on Civil and Political

	Rights
INGO	International Non - Governmental Organization
IPC	Indian Penal Code
IT	Information Technology
Ker	Kerala
Ltd.	Limited
NCRB	National Crime Records Bureau
NGO	Non - Governmental Organization
NHRC	National Human Rights Commission
Ori	Orissa
P&H	Punjab and Haryana
PAN	Permanent Account Number
PIL	Public interest litigation
POTA	Prevention of Terrorism Act
PUCL	Peoples Union for Civil Liberties
PUCLDR	Peoples Union for Civil Liberties and Democratic Rights
PUDR	Peoples Union for Democratic Rights
Punj	Punjab
Raj	Rajasthan
SC	Supreme Court
SCC	Supreme Court Cases
SCR	Supreme Court Reports
Sec.	Section
SSN	Social Security Number
TADA	Terrorist and Disruptive Activities (Prevention) Act
U.K.	United Kingdom
UAPA	Unlawful Activities Prevention Act
UDHR	Universal Declaration of Human Rights
UIDAI	Unique Identification Authority of India

UN	United Nations
UP	Uttar Pradesh
US	United States
WB	West Bengal
WP	Writ Petition

CHAPTER 1

INTRODUCTION

“Sometimes, the scandal is not what law was broken, but what the law allows.”

-Edward Snowden

The safety and security of a country have always been of paramount importance to every state presently in existence. Security isn't something which has become something of grave consideration as of this day; it has always been a thing of remarkable importance since the very inception of human civilisation. All the mythical stories we have heard, all the legends that we have read, all the stories have been shared with us, all the kings and empires that history can trace back to, there is only one thing which connects every one of them, soldiers and wars. Be it, Jesus Christ, be it the Roman Empire, be it the Spanish Inquisition, and be it Zeus and his war with the Titans, soldiers, and wars were a part of all of them. This shows that humanity itself is naturally inclined towards having a sense of security no matter whether it is in their person, their house, their city, or their whole empire. Even Abraham Maslow, in his renowned Maslow's Need Hierarchy Theory, puts security needs just above the basic physiological needs of a person in his pyramid of needs, thereby showing how important it always has been to the mankind.

What's even more profound is the fact that entire empires have been started from dust, and existing empires have fallen to dust just over the issue of security. Even the Japanese started invading China and parts of Korea because they were afraid that they will themselves be attacked if they did not do so. While the ways have always differed as to what a country perceived a viable way to secure itself, most of the methods which have been used since time immemorial cannot be used in the present day scenario. As civilized human beings, we always have to learn from our past and the mistakes we've made and strive to evolve from them. We have several accords that prevent us from

doing terrible acts against an individual and crimes against humanity. Conventions such as the United Nations Convention against Torture (UNCAT), Geneva Conventions, Nuremberg Principles, etc. have put all the necessary checks and balances to ensure States don't cross boundaries when it comes to the treatment of prisoners who have harmed or pose a threat to the security of the state.

While these Treaties and Conventions give a sense of pride and safety to individuals, their real-life implementation shows a completely different ground reality altogether. After the passing of the Geneva Convention back in 1949, states vowed not to do any act which violated the Geneva Convention in any way, shape, or form. The United States of America, who is a signatory and has ratified the Geneva Convention, has been a forerunner when it comes to the gross violations of the said conventions. The most horrifying example of the same would be when the United States Senate Select Committee on Intelligence investigated the acts of the Central Intelligence Agency, while it investigated all known suspects who had any connection to the September 11 attacks on the World Trade Centre. The horrifying acts which were committed by the CIA were revealed in the Committee Study of the Central Intelligence Agency's Detention and Interrogation Program.¹ It showed that the CIA have used methods such as Anal Rehydration, Waterboarding, Mock Deaths, Sleep Deprivation amongst other cruel and inhumane acts to question the known suspects of the 9/11 attacks.

Other Countries such as the Russian Federation, People's Republic of China, North Korea, etc. have also been, on numerous occasions criticized by other countries and International Organizations for their blatant disregard for the human rights of their citizens. As Nelson Mandela has very rightly put forward, "*To deny people their human rights is to challenge their very humanity*". Countries cannot, and should not commit any act which even remotely poses any such threat to individuals.

¹ *Report of the senate select committee on intelligence committee study of the Central Intelligence Agency's Detention and Interrogation Program*, 113TH CONGRESS 2ND SESSION S. REPORT (2014) <https://www.intelligence.senate.gov/sites/default/files/documents/CRPT-113srpt288.pdf>

While its counterparts around the globe have always been subject to speculation over the disregard for human rights, India has always managed to be away from such kind of defamatory criticism. The Indian Government, since its independence, has lived by the words of M.K. Gandhi who said that *“The greatness of humanity is not in being human, but in being humane.”* India has always stood up for what’s right, and even in the darkest of times when individual liberties were threatened, the Supreme Court of India has always stood firm in protecting the rights of those who are threatened.

That being said, it never was the case that India’s past has been as white as a dove when it came to liberties of an Individual. To protect the sovereignty and integrity of the nation, India has also at times gone to lengths, while having little to no disregard for individual liberties and freedom. The first stain of blotted ink on India’s clean past happened back in the year 1967, when the Government of India decided to pass the Unlawful Activities (Prevention) Act, 1967, which we more prominently have known as the UAPA. While the 1967 act looks like a piece of cake in front of the act which stands today, it still had some horrifying provisions inside of it, which gave the Government unfettered powers to act on their will if a certain crime had been committed and was punishable under the said act.

The UAPA was legislated solely for the reason that there was a growing sense of discontentment amongst the population of India, which wanted to secede from the territory of India. The country as we see today still didn’t look like it back in 1967, a handful of states were yet to join, and those who joined had been voicing their concerns throughout. The State of Tamil Nadu back then already was extremely disappointed with the Government of India holding back on its promises, and taking advantage of this disappointment, the DMK party went on to contest the elections. The party stated in its manifesto that if elected to power, the DMK would work to secede the state of Tamil Nadu from India, and create an Independent Country for the Tamil. This scared the Government even more since it had already lost a part of its territory in Aksai Chin after the 1962 Sino-Indian War. Therefore, the act which was legislated simply put forward that any person who commits and “Unlawful Activity”

shall be punishable under the said act. Also, any person who is a member of an “Unlawful Organization”, shall be punishable under the said act.

The issue with the legislation was the fact that nowhere in the act was it clearly defined what constituted as an “Unlawful Activity”. What was stated, was the fact that any act, which threatened the Sovereignty and Integrity of the Nation would be considered as an Unlawful Act, thereby leaving it entirely in the hands of the Government to decide which act was unlawful and which wasn’t. Furthermore, what was even scarier was the fact that the said act allowed arrests without warrants and preventive detention for up to 180 days to those who have been charged with this act. This marked the beginning of gross human rights violations under the said act, which would further go on to become one of the most draconian laws in India. Hence, this led to the Government of India having a scary arbitrary power in its hands. As George Washington has rightly said, *“Arbitrary power is most easily established on the ruins of liberty abused to licentiousness.”*

What started with just the UAPA went on and spread like poison in the hands of the Indian Legislature, Years after legislating on the UAPA, when faced with a similar issue of internal security. This was after the Operation Blue Star was conducted by the government in the State of Punjab. The Government passed the notorious Terrorist and Disruptive Activities Act, 1987, which more prominently came to be known as the TADA. However, the act was so grossly misused by the authorities that it had to be repealed merely 6 years after it was legislated.

The act provided that a person can be detained for up to 1 year without any formal charges being pressed on him. The Act further provides that a detainee can be in the custody of the police for up to 60 days, and post than even, he needs not to be presented before a magistrate, but an Executive Magistrate.² Furthermore, the act reverses the presumption of innocence, stating that a person caught under this act is presumed guilty until his innocence is proven otherwise.³ Lastly, any person who is tried under this act cannot appeal

² Terrorist and Disruptive Activities (Prevention) Act, 1987, S 20.

³ The Terrorist and Disruptive Activities (Prevention) Act, 1987, S 21.

anywhere, except to the Supreme Court of India.⁴ For reasons such as this which are so immoral, the act was allowed to lapse in 1995 when it was due for renewal. During the 7 years TADA remained in force, 76000 people were arrested in India under the act.⁵

After TADA lapsed, and the Indian Parliament was bombed in the year 2001, the need arose for a new law to prosecute those who have been found guilty of the said offense. This led to the Indian Legislature passing the Prevention of Terrorism Act, 2001, which more prominently came to be known as POTA. Just like TADA, POTA also had numerous provisions that allowed for blatant misuse of powers. POTA also had the provision for holding a person in custody for up to 180 days without any filing of the charge sheet. Further, the laws in India do not accept any confession made to a police officer as evidence and allow it to be rebutted in a trial. *“This was however not the case in POTA, and every confession made to a police officer is admissible and can be used against a person in trial. POTA was misused heavily by the government, and the police itself misused the act to torture and humiliate prisoners.”*⁶ As Norman Finkelstein has rightly put, *“No conditions justify torture”* and therefore when the government at the center changed, POTA was accordingly repealed.

The issue in hand, however, has also been the fact that while states have blatantly used their arbitrary powers to interfere with the rights of a human being, one right which has always gotten stepped upon during all of this is the right to privacy of an individual. The privacy of a person is always something that is valued the most. As Edward Snowden has said, *“Privacy isn’t about something to hide, it’s about something to protect”*. All the legislation which have been laid forward above has always had one thing in common, which is a

⁴ The Terrorist and Disruptive Activities (Prevention) Act, 1987, S 19.

⁵ ZAIDI, S. HUSSAIN, BLACK FRIDAY – THE TRUE STORY OF THE BOMBAY BOMB BLASTS. (Penguin Books 2003) ISBN 978-0-14-302821-5.

⁶ Nitya Ramakrishnan, *Tortured, Humiliated, But Unbroken: An Interview With S.A.R. Geelani*, The Wire, Oct. 25, 2019. <https://thewire.in/rights/sar-geelani-custodial-torture-nitya-ramakrishnan> (Last Visited: 01st August, 2020).

blatant disregard for the privacy of an individual. The forerunner in this section, however, remains the UAPA.

An instance of the UAPA being misused of such a horrendous act would be when the Delhi Police barged directly into the home of the AISA President Kanwalpreet Kaur and seized her mobile phone stating that it was required as a part of the investigation under the Delhi Riots. When she was handed the seizure memo, along with a bunch of charges, a few changes were also placed under the UAPA for seizing her mobile phone.⁷

The UAPA has also been criticized by the United Nations Special Rapporteurs for violating the privacy of a said individual. The amended Act allows for searches, seizures, and arrests based on the “personal knowledge” of police officers without a written validation from a superior judicial authority. The police are empowered by the amendments to enter the premises on a person on the mere suspicion of her being part of an “unlawful association”. The police have the power to examine the books, and other properties of the accused and also make inquiries against her. This, the statement declares, is a clear violation of the right to privacy as per India’s international law obligations.⁸

The Act also interferes with the privacy and liberty of individuals contravening the provisions which protect against arbitrary or unlawful interference with a person’s privacy and home. The Act allows for searches, seizures, and arrests based on the ‘personal knowledge’ of the police officers without a written validation from a superior judicial authority.⁹ This interferes with the privacy and liberty of individuals which is not only by a fundamental right but also contravenes the provisions of the International Convention on Civil and Political Rights (ICCPR)”, which protects against arbitrary or unlawful interference with a person’s privacy and home.

⁷ Special Correspondent, *Police bid to intimidate Kawalpreet, claims AISA*, THE HINDU (Apr. 29, 2020). <https://www.thehindu.com/news/cities/Delhi/police-bid-to-intimidate-kawalpreet-claims-aisa/article31462959.ece>

⁸ Ujjaini Chatterji, *UN Special Rapporteurs express concerns over UAPA*, THE LEAFLET (May 18, 2020). <https://theleaflet.in/un-special-rapporteurs-express-concerns-over-uapa/>

⁹ Aakar Patel, *UAPA (Amendment) Bill 2019 violates the very international laws it quotes, defies principles of natural justice*, FIRSTPOST, (Aug. 3, 2019) <https://www.firstpost.com/india/uapa-amendment-bill-2019-violates-the-very-international-laws-it-quotes-defies-principles-of-natural-justice-7104391.html>

The Right to privacy of an individual has to be protected, and so has been time and again said by the courts. There have been numerous judgments wherein the courts have asked the government to make laws in accordance with protecting the privacy of an individual, but the government has somehow or the other managed to get away without actually doing something to protect the rights of an individual. The Supreme Court has stressed upon the fact that “it is entirely for the Central Government to make rules on the subject of interception but till the time it is done the right to privacy of an individual has to be safeguarded.”¹⁰

“If the right to privacy has to mean anything, it is the right of an individual, single or married, to be free from unwarranted government intrusion.” These were the words of William Brennan Jr. when asked about the views on privacy. Well, these words make more sense now than ever, when asked about the state of privacy in India. If we have to on the morally correct side of history, we cannot let any act, not even national security supersedes the privacy of an individual.

¹⁰ People’s Union of Civil Liberties Vs. Union of India, AIR 1997 SC 568

CHAPTER 2

RESEARCH METHODOLOGY

2.1. Research Background/Introductory

The Term Privacy, as defined by the Black's Law dictionary refers to "the right that determines the non-intervention of secret surveillance and the protection of an individual's information. It is split into 4 categories:

- (1) Physical: An imposition whereby another individual is restricted from experiencing an individual or a situation.
- (2) Decisional: The imposition of a restriction that is exclusive to an entity.
- (3) Informational: The prevention of searching for unknown information and
- (4) Dispositional: The prevention of attempts made to get to know the state of mind of an individual."

Now in simple terms, if we talk about the right to privacy then it means the right to be let alone or the enjoyment of living one's life without any kind of unnecessary intrusion or interference. It plays a very important part in every individual's life and recently the Supreme Court has also considered this right as the fundamental right of every citizen. Article 21 of the Indian constitution's scope has been expanded to include the right to privacy as a fundamental right (the given article states that "no person shall be deprived of his life or personal liberty except according to the procedure established by law".) Since the ambit of this Article is very wide and a lot of interpretations have been done by the Courts, therefore, this time after so many contradictory judgments, finally we can say that right to privacy is now recognized as a fundamental right under the fundamental right to life and liberty.

The right to privacy has been a very debatable topic since the independence of our country and this concept has majorly evolved or developed through various judgments over the last seventy years of our independence as there is no specific provision for this right guaranteed under the Constitution. Before

the 2017 judgment of *Justice K.S. Puttaswamy vs. Union of India*¹¹, the right to privacy was not considered as our fundamental right. In the two earlier judgments of *MP Sharma v Satish Chandra*¹² in 1954 and *Kharak Singh vs State of Uttar Pradesh*¹³ in 1962, it was held that the right to privacy does not fall within the ambit of fundamental rights guaranteed under the Constitution. In the United States Fourth Constitutional Amendment, the protection from unreasonable searches and seizures was given to its citizens. In the former case, concerning this contention, it was ruled that it can't be read into the Constitution of India and the court held that "a power of search and seizure is in any system of jurisprudence, an overriding power of the State for the protection of social security and that power is necessarily regulated by law. When the Constitution makers have thought fit not to subject such regulation to constitutional limitations by recognition of a fundamental right to privacy, analogous to the American Fourth Amendment, we have no justification to import it, into a different fundamental right by some process of strained construction. Nor is it legitimate to assume that the constitutional protection under Article 20(3) would be defeated by the statutory provisions for searches." In the latter case of *Kharak Singh*, he filed a writ petition that his fundamental rights under Article 19 (1) (d) and Article 21 of the Constitution has been violated as he was kept under six measures of "surveillance" as per Chapter XX of the Uttar Pradesh Police Regulations. The Court, in this case, held that "the right of privacy is not a guaranteed right under our Constitution, and therefore the attempt to ascertain the movements of an individual is merely a manner in which privacy is invaded and is not an infringement of a fundamental right guaranteed in Part III (fundamental rights)".

For so many years these judgments have been followed and finally, in 2017, the Supreme Court considered that the right to privacy of an individual is equally important as other fundamental rights under Part III of the Constitution. Therefore, the present ruling of the Apex Court considers the right to privacy as our fundamental right.

¹¹ AIR 2017 SC 4161.

¹² AIR 1954 SC 300.

¹³ AIR 1963 SC 1295.

2.3. Aim(s)

In the dissertation, by highlighting the importance of the right to privacy, the researcher will focus on every possible dimension and scope of this right and how when cumulatively read and understood with the national security laws and acts, it stands the test of time and can cope up with the growing need of privacy and existing requirement of security of the nation. It has been already stated in the introduction that the right to privacy is now the fundamental right of every citizen in India, the development of this aspect will be discussed. Privacy of a citizen could include a lot of aspects in which they want their personal space and no unnecessary or unreasonable intrusion of public authorities like telephone tapping, police surveillance, the medico-technical use of interrogation techniques like narco-analysis by the police and search and seizure powers of different state agencies. It was a very debatable topic of discussion, before the Supreme Court considered it a fundamental right under Part III of the Constitution, as to what extent this right should be granted to the citizens. The question of the right to privacy of the citizens has been discussed in many cases. The analysis of the judicial trend is also important because it will give an idea of the judicial interpretation of the courts concerning the right to privacy. Likewise, it is important to protect our nation and government sometimes takes harsh steps which at times are violating personal liberty, freedom, and privacy of the citizens, in this paper the researcher has tried to analysed the said situation by analysing the recent amendments and relevant legislations and has tried to come up with the method for harmonizing both the interests so that one is not violating the other and can exist in the same space, while sometimes overlapping but never encroaching the space of the other right.

The right to privacy is now a fundamental right under the Constitution but if we talk about any specific legislation or Act which deals with the privacy laws in India then we will not find any Act in force that deals with the privacy rights of Indian citizens. In the Constitution also, there is no Article talking specifically about the privacy rights of the citizen. It has been made a fundamental right under the ambit of Article 21. Although making it a fundamental right is one of the major steps taken by the Indian judiciary

concerning privacy laws but still there is a need of proper legislation which could specifically talk in detail with matters connected to privacy and remove few ambiguities that have been arising since the privacy right became our fundamental right, this is more important considering that lack of stringent and well-established laws leaves a lot of space for the autonomy of acting in whatever way the government deems fit in the name of protecting the national interest and national security. If we look minutely into few Acts then few provisions cover the privacy of Indian citizens but this is restricted to a certain limit. For example, the Information Technology Act, 2000, provides for provisions regarding the protection of digital privacy and data security of the citizens. So, this issue will also be discussed in the dissertation.

One of the biggest issues that are in question, after the Supreme Court declared the right to privacy as a fundamental right, is the issue of Aadhar program and the security threat it posed while also being called as the black mark on the face of privacy as a fundamental right. The question arises is the constitutional validity of it including the Aadhaar Act, 2016. It makes Aadhaar compulsory for every citizen and the government wants to make mandatory linking of Aadhaar to avail welfare schemes and other services run by the government. The government wants every citizen to compulsorily link their mobile number, bank accounts, PAN, etc.. The Aadhaar contains a lot of personal information like the demographic information and biometric information which could be misused in some circumstances by others if not kept confidential. The risk of the data leak is also associated as Aadhaar applies to commercial purposes and the private parties can have access to the data and as already discussed; we have no privacy laws in our country which could deal with these kinds of situations. Therefore, these are a few problems that are required to be addressed in detail and hence form a very crucial part of the dissertation.

It is also necessary to understand whether there are any demits or drawbacks in granting the right to privacy as a fundamental right. Although fundamental rights are also subject to certain restrictions and are not absolute rights in comparison to a fundamental right and a statutory right, the fundamental rights hold more weightage and importance. In the absence of the statutory legislation regarding the right to privacy and directly making it a fundamental

right seems that some loopholes or ambiguities could be there. To understand this dimension of the right to privacy, it is required to get into the details of related cases and legislations. The legislations such as POTA and UAPA are covered and detailed analysis of how in national security, the right of privacy is often pierced.

2.4. Objectives (s)

1. To critically analyse the importance of the right to privacy in India.
2. To understand the right of privacy in the ambit of the fundamental right to life and liberty guaranteed under Article 21 and all the other possible constitutional dimensions and scope.
3. To critically analyse the judicial trend related to the development of the right to privacy in India.
4. To do a comparative study of the laws related to privacy rights in other countries and India and the security laws
5. To analyze and understand the need for specific legislation on privacy laws in India to understand the loopholes to prevent the encroachment of the right in the name of national security
6. To do a critical analysis of all the related judgments and legislations to find out the loopholes or the negative aspects, if any, in making the right to privacy our fundamental right and Importance of the security legislations present in the country.
7. To discuss whether every aspect of the right to privacy should be considered to be our fundamental right or whether there are still some aspects of privacy which are not considered to be the fundamental rights of the citizen and whether it is okay to surrender all rights relating to privacy in the name of national security.

8. To analyze the Legislations relating to national security and their loopholes which they exercise to pierce the right to privacy by understanding and analyzing real-life incidences.

2.5. Scope and Limitations

The purpose of the study is to establish a nexus between the right to privacy of an individual and the National Security of the state and come to a conclusion that how both of them are important in their ways and we cannot overlook one in the name of other. It focuses on the areas wherein the problem lies and the issues arise, relating to the encroachment of the right to privacy, which is now considered to be a fundamental right.

The topics covered ranges from the Data privacy bill, Important judgments which change the course of the debates under privacy as a right, The national security legislations such as UAPA, in respect to the violation of fundamental rights, along with the right to privacy, the mobile application ban imposed by India on china, due to the arising state of conflict on the borders and to protect data, the need for data localization The method of the study is doctrinal.

2.6. Literature Review

Books

1. Basu, Durga Das, “*Commentary on Constitution of India*”

According to the author, since the supreme court of India has already inculcated Right to Privacy in the Right to life and Personal liberty as stated under Article 21 of the Indian constitution, therefore, the proposal of the author that a new Article relating to the same, namely 21-B should be inserted in the constitution.

2. Ravinder Kumar and Gaurav Goyal, “*The Right to Privacy in India: Concept and Evolution*”.

In this book, the authors have carefully analyzed whether the right to privacy gives the right to invade someone's privacy and the jurisprudence behind the right.

3. Jain, M.P., *Constitutional Law: Fundamental Right*, Lexis Nexis, 7th end. 2014.

Only a reasonable claim to privacy can be sustained under the custom. In *Syed Habib vs. Kamal Chand*, the Rajasthan High Court pointed out that a customary

Easement of privacy to be valid under Article 19 (1)(f) has to be reasonable as required by Article 19(5).

4. S.K. Sharma, "*Privacy Law: A Comparative Study*"

The book studies every aspect of the subject minutely. Freedom of information act and the privacy act of the U.S.A. have been analyzed. All the relevant case laws right from the case-law of Griswold to the case of Govind have been deeply studied. The case laws relating to the right to privacy and infringement of privacy as seen in other countries have been analyzed in the detail.

5. Marta Otto, "*The Right to Privacy in Employment: A Comparative Study*"

According to the author, the term 'privacy' and the concept of privacy gained and garnered prominence around the globe, but in the field of law and the legal arena, it is still looked upon as a state of disorganization and in disarray. To put in inside the box of a legal framework where the encroachment and overlapping of privacy with other arenas and problems relating to the modern society which are although complex is also seen more frequently are observed. The mentioned problems, according to this book can be solved by the development only lead by the holistic approach, it is also discussed that the approach should be such that it addresses the issue of not only just for the contemporary regulations but also the conceptualization and common perception of employees' privacy.

6. Richard A. Glenn, *“The Right to Privacy: Rights and Liberties Under the Law”*

This book features a thorough introduction to privacy law, covering landmark cases, important themes, historical curiosities, and enduring controversies.

7. Adam Carlyle Breckenridge, *“The Right to Privacy”*

According to the author, the Right to Privacy is predicated upon the assumption as well as the belief that the individual has the right to establish the degree to which he wishes to share of himself with others and has control over the time, place, and circumstances during which he communicates with others; that he has the right to pull out of or engage as he sees fit; and therefore the right to regulate the dissemination of data and information about himself.

8. Brandon Garrett, *The Right to Privacy*

According to the author, our right to privacy isn't specifically protected by the Bill of Rights, but it's implied in various ways within the Constitution. This book examines just how extensive or restricted that right is, as interpreted over the years by our system.

9. David L. Hudson, *The Right to Privacy*

According to the author, the Right to Privacy, a globally garnered concept, examines issues concerning the media's got to gather news, the government's power to conduct surveillance, employers' ability to watch and control the workplace, and therefore the ways technology has challenged this right.

10. Caroline Kennedy and Ellen Alderman, *The Right to Privacy*

According to the authors, although the word privacy doesn't appear within the Constitution, most folks believe that we have an inalienable right to be left alone. They surveyed many recent cases during which ordinary citizens have come up against the intrusions of state, that is the government, businesses, journalism, and their neighbors.

Articles

1. Vrinda Bhandari and Renuka Sane, *“Towards a privacy framework for India in the age of the Internet”*.

In this article, the analysts and academicians have put forth a defense for India to authorize a privacy protection law. Such a law would characterize key terms, administer the privileges and privacy of clients, detail the commitments of the State, set down protection standards and exemptions, give direction on settling security clashes (for example, by applying a European proportionality test) and would depict different review and remuneration components.

2. Namit Oberoi, *“The Right to Privacy: Tracing the Judicial Approach Following the Kharak Singh Case”*.

According to the researcher, it's evident that there's an implied, unremunerated, but judicially evolved and recognized right to privacy under the Indian Constitution. Although the rulings of the Supreme Court within the cases of MP Sharma and Kharak Singh, denied the existence of any right to privacy, in the case of Rajagopalan, the smaller benches and People's Union for civil liberties expressly indicate the existence of such a right. The shift in judicial interpretation is most notably observed following the Maneka Gandhi case, wherein this right is recognized, subject to legal restrictions satisfying what is required and wanted as laid down within the Maneka Gandhi case.

3. Anubhav Khamroi and Anujay Shrivastava, *“The Curious Case of Right to Privacy in India”*

According to the researcher, it can be duly established that not only the Judiciary but also the Legislature at certain instances have recognized the essential Right to Privacy and the need to make it a statutory right.

4. Aashit Shah and Nilesh Zacharias, *“Right to Privacy and Data Protection”*.

According to the researcher, a legal framework needs to be established setting specific standards relating to the methods and purpose of assimilation of personal data offline and over the Internet. Consumers must be made aware of voluntarily sharing information and no data should be collected without

express consent. The future of India's trade depends on striking an effective balance between personal liberties and secure means of commerce.

5. Daniel J. Solove, "*Conceptualizing Privacy*"

In this Article, Professor Solove develops a new approach to conceptualizing privacy. He begins by examining the existing discourse about conceptualizing privacy, exploring the conceptions of a wide array of jurists, legal scholars, philosophers, psychologists, and sociologists. Solove contends that the theories are either too narrow or too broad. With a few exceptions, the discourse seeks to conceptualize privacy by isolating one or more common "essential" or "core" characteristics of privacy. Expounding upon Ludwig Wittgenstein's notion of "family resemblances," Solove contends that privacy is better understood as drawing from a common pool of similar characteristics.

6. Adam D. Moore, "*Privacy: It's Meaning and Value*".

According to the researcher, privacy is valuable for beings like us. The ability to regulate access to our bodies, capacities, and powers and sensitive personal information is an essential part of human flourishing or wellbeing. Modern surveillance techniques, data mining efforts, and media coverage are opening up private lives for public consumption. Technological advancements in monitoring and data acquisition are forcing us to rethink our views about the value of privacy. The unexamined life, as Socrates once said, is not worth living, but neither is the life examined by police or corporations, or the life open to inspection by anyone for any reason.

7. Neeraj Grover, "Right to Privacy in Digital Age: Evolving Privacy Laws and Their Applicability to Social Media".

According to the researcher, it is clear that the law of privacy is still in its benign stage. It may efficiently cope up with privacy problems that exist in the real social world but to handle privacy in the cloud digital media, it needs a more rigorous approach. "The question shouldn't be whether the user expected that information about him should remain private after sharing it with so many people"⁶⁹ because even despite making "rational choices", users are often met with situations they never really foresaw and consented to.

8. Gautam Bhatia, “State Surveillance and The Right to Privacy in India: A Constitutional Biography”.

According to the researcher, it is unclear how the Court will rule on a CMS/surveillance challenge. One thing is clear, though: the privacy law jurisprudence that it has developed over the last fifty years provides it with all the analytical tools to fulfill its constitutional mandate of protecting civil liberties. Consistent with the narrow tailoring test, the Supreme Court ought not to allow the government to baldly get away with asserting a national security interest but require it to demonstrate not only how national security is served by dragnet surveillance, but also how dragnet surveillance is the only reasonable way of achieving national security goals.

9. Afshan Nazir and Ayush Gupta, “*Right to Privacy: Fundamentally Ours*”.

According to the researchers, Freedom of life and liberty is incomplete without our ability to be who we are away from the glare of those who wish to overpower us. The “right to privacy” is a fundamental right eventually and we can now go running to top court if ever someone peeks nose into our matters unnecessarily. The verdict on ‘Right to Privacy’ has again widened the horizons of Article 21 after Maneka Gandhi & Mohini Jain cases.

10. Suhrith Parthasarathy, “*Privacy, Aadhar, and the Constitution*”.

In this article, the researcher argues that the present clash over the right to privacy must encourage us to think more deeply about the deficiencies of our Constitution. We must engage in a battle to not only have the Constitution interpreted in an appropriate democratic spirit but also to have inserted into it certain rights and liberties that require explicit elucidation.

11. Nooraneeda Mutalip Laidey “Privacy v National Security, where do we draw the line”?

Privacy is sacred and would normally be expected and preserved by an individual. Online privacy is no longer about the right to be left alone but also includes the right not to be monitored. However, with the revelations made by United States National Security Agency former employee Edward Snowden

that the government is spying on internet communications, individuals' privacy can no longer be expected.

12. Entry 2A of List I and Entry 2 of List II, Seventh Schedule:

The petitioner put forth an argument based on two basic features of the Indian Constitution, in case of Committee for Protection of Democratic Rights v. State of West Bengal, 2001 Cri.L.J. 2307, that the basic features are federal setup and separation of powers. The state legislature has jurisdiction over police matters as per constitutional and statutory provisions. It is to state that without the consent of the concerned state government, the parliament cannot encroach upon it 18.

13. Ruma Pal, (Rtd. SC, J.) In his "Judicial Oversight or Overrich":

The Constitution allows for parallelism of power, with hierarchies between the three organs in particular fields as stated by retired Supreme Court Judge Ruma Pal. That the subject to checks by the other two, which must be maintained and balanced by each organ

14. In ADM Jabalpur v. Shiva Kant Shukla case:

In the Constitution and statute law, if the right to personal liberty is limited by any limitations other than those expressly contained, the Supreme Court sought to determine. Article 21 is not the sole repository of the right to personal liberty, without the authority of laws no one shall be deprived of his life and personal liberty, as observed by Khanna Judge of the Supreme Court. It flows equally from statutory law like the penal law force, and not merely from common law in India

15. Dicey, In his "Law of the Constitution":

Dicey in his book law of the constitution mentioned as in the earlier editions of Dicey that the rule of law is an essential part of accountability, of course, he modified in later editions there is something inconsistent with the rule of law,

therefore, that conferment of any discretion tends to arbitrariness. The conferment of some discretion for application to the facts of a given case is something you cannot do away with, but then, as when time passed that it was realized by Dicey

16. Birutė Pranevičienė *“Limiting of the right to privacy in the context of protection of national security”*

“For the last several decades, ensuring human rights and national security has remained an important goal and a condition for the existence of every state. The interests of national security often presuppose the need to narrow some natural rights, such as, for example, the right to privacy, the right to secrecy of communication, etc. The traditional concept of security is related to ensuring national security. According to the traditional concept of security, the state is considered the main object of security; therefore, the states mainly focus on external threats. It is stated that the most important thing is to protect the state from external aggression, ensure the protection of state borders and institutions. The protection of human rights is ensured simultaneously. It is, however, observed that a secure state does not necessarily mean that the citizens of the state are secure. The security of a person is under threat due to limitations imposed on human rights while seeking to ensure national security. An issue related to the protection of human rights is presented in the article when limitations on a person’s right to privacy are foreseen for the protection of national security.”

2.7. Research Questions

Issue No. 1) Whether National Security Agencies pierce the Right to Privacy of Citizens under the excuse of National Security?

Issue No. 2) whether judicial Review is effective as a deterrent towards abuse of fundamental rights by the government?

Issue No. 3) whether the amendment in UAPA Breaches the right to privacy of citizens?

Issue No. 4) what are all the privacy laws can be adopted from our counterpart countries, facing the similar dilemma of whether putting national security above right to privacy or vice-versa and is there any viable way of harmonizing the both interests

Issue No. 5) how relevant are the Chinese Apps Ban imposed by India, and whether is it lawful by the WTO treaty which India is a signatory of. Was there an imminent and grave threat of data leaking and national security matter or not?

2.8. Research Methods applied to test the hypothesis/hypotheses

The research work that has been conducted has been finished with the assistance of doctrinal technique which incorporates the lawful structure and legal frameworks, a comparative study has been carried out in understanding the concept of limited government and security legislation through the privacy laws in India and around the world. The researcher has made a report on Limited government and security enactment, with the emphasis on the privacy protection laws in India and how for the sake of national security, the legislature is going over the edge with the surveillance and encroachment of the laws essential to the people.

The theory of the researcher and the hypotheses formed by the researcher is that the assurance and protection of the individual freedom and liberty from the intervention and the smooth running of a fair and democratic government need separation of power in a check and balance structure yet not in an unbending and rigid structure with changing nature of the general public and society

It is to maintain the limited government in the country and how further development of the same is important so that judicial review can be used as an important tool and be an effective deterrent towards the arbitrariness with which certain legislations are formed. The paper sheds light upon the following and they are discussed at the lengths to reach a conclusion that is fair, just, and reasonable.

For this dissertation, it is assumed that every citizen is entitled to have the right to privacy. Every right comes with liability and every freedom granted to a citizen is subject to some kind of restriction which is in the interest of the public in large. It seems quite obvious that the right to privacy is such a right that could not be granted to the citizens and at some of the other points, it will be subjected to certain restrictions depending on the circumstances. With time, the courts started considering the importance of this right. As there is no specific legislation, therefore, it was always the responsibility of the courts to understand and consider this aspect. For as long as one can remember, it was a common notion and the precedent which clearly emphasized the fact that the right to privacy is not considered being a fundamental right. Considering that India has the second-largest population and is still a developing country, where some people do not even have access to the basic facilities like food, water, shelter, etc. it was considered unnecessary by the courts to take into consideration the privacy rights and hence it took a long time for the Supreme Court to finally recognize the right to privacy as our fundamental right.

The recent step was taken by the Supreme Court in contradiction to the earlier judgments and making it a fundamental right shows the growth of the Indian judiciary. This change brought along with it certain questions especially regarding the constitutional validity of Aadhar. Also, it is presumed that in absence of a statutory right to privacy or any other legislation on the right of privacy, the fact that it is our fundamental right, brings few questions in mind concerning the loopholes associated with it. So, there is a presumption of demerits or drawbacks which could be cleared only after a detailed study of all the dimensions and scope of the right to privacy. But keeping the negative aspect aside, this step is more of a positive change, as other developed countries consider this right equally important as other rights of the citizen and have legislations and laws to deal with the different matters related to the privacy laws. India finally has a law on right to privacy so this is one of the major steps taken by the Supreme Court recently. Since steps are been taken for the Right to privacy as a fundamental right, the debate arises that is this right just given to the citizens and can be infringed at the whims and fancies of

the ruling government or will there be sufficient laws to protect the interest of the people and their newfound right in the name of privacy.

2.9. Research Design

The study design is non-observational. First, the existing literature on the scheme was looked upon, problem and hypothesis were drafted. After the collection of data and analysis, a conclusion has been drawn on the outcome of the study undertaken.

2.9.1 Approach

A qualitative research approach was adopted to collect the data for the research work. The qualitative data refers to “textual data” and refers to the non-numerical data.

2.9.2 Tools of Data Collection

(a) Secondary Data

To understand the purpose behind the new data protection bill and the existing laws relating to privacy and National security and how they are in conflict with each other and to find a solution based scheme and to comprehend the views of the judiciary concerning various online databases, newspaper articles and court judgments were referred.

CHAPTER 3

UNDERSTANDING PRIVACY VIS-À-VIS STATE POWER

“In 1890, in a classic article that many scholars now regard as a seminal work on privacy, Samuel Warren and Louis Brandeis described privacy in terms of *being let alone* or being free from intrusion.” “This conception of privacy, as non-intrusion, is also evident in the writings of two U.S. Supreme Court justices: Louis Brandeis in *Olmstead v. the U.S.*¹⁴ and William Brennan in *Eisenstaedt v. Baird*.¹⁵ “We should first note that some versions of the no intrusion theory tend to confuse the condition (or content) of privacy with a right to privacy.” “This confusion is especially apparent in the writing of no intrusion theorists, such as Brandeis, who defines privacy as the right to be let alone¹⁶”, and Brennan, who describes privacy as the “*right of the individual . . . to be free from unwarranted government intrusion*”¹⁷

According to Fried, “*Privacy is not simply an absence of information about us in the minds of others, rather it is the control over the information we have about ourselves.*”¹⁸ Miller embraces a version of the control theory when he describes privacy as the individual’s ability to control the circulation of information relating to him.

¹⁴ 277 U.S. 438 (1928).

¹⁵ 405 U.S. 438 (1972)

¹⁶ *Olmstead* 475, Brandeis dissenting

¹⁷ *Eisenstaedt v. Baird* (p. 453).

¹⁸ KENNETH EINAR HIMMA and HERMAN T. TAVANI, *THE HANDBOOK OF INFORMATION AND COMPUTER ETHICS*, (John Wiley and Sons, Inc.)

We observe privacy with such notions as liberty, solitude, autonomy, and secrecy. Nissenbaum points out that although we have privacy norms (that is, explicit privacy laws and informal privacy policies) that protect personal information considered to be intimate and sensitive for example, medical records and financial records normative protection does not generally extend to personal information considered to be neither sensitive nor intimate. She also indicates that most normative accounts of privacy have a theoretical blind spot when it comes to questions about how to protect personal information in public contexts or in what she calls spheres other than the intimate. Her analysis of this problem illustrates some of the controversies associated with the practice of mining personal data from public sources. At first glance, such a practice might seem innocuous because of the public aspect of the data involved.

“A definite legal definition of ‘privacy’ is not available. Some legal experts tend to define privacy as a human right enjoyed by every human being by his or her existence. It depends on no instrument or charter. Privacy can also extend to other aspects, including bodily integrity, personal autonomy, informational self-determination, protection from state surveillance, dignity, confidentiality, compelled speech, and freedom to dissent or move or think. In short, the right to privacy has to be determined on a case-by-case basis. Privacy enjoys a robust legal framework internationally.”

“Article 12 of the Universal Declaration of Human Rights, 1948 and Article 17 of the International Covenant on Civil and Political Rights (ICCPR), 1966, legally protect persons against arbitrary interference with one’s privacy, family, home, correspondence, honor, and reputation. India signed and ratified the ICCPR on April 10, 1979, without reservation. Article 7 and 8 of the Charter of Fundamental Rights of the European Union, 2012, recognizes the respect for private and family life, home and communications. Article 8 mandates the protection of personal data and its collection for a specified legitimate purpose.”

“Privacy is not a concept like other rights. Moreover, our notions of privacy have changed and will continue to change. If there is one major catalyst for this change, it has been technology. Built homes are a simple example of how we develop a sense of privacy which is influenced by technological development. Once we have a conception of home, we also have conceptions of a bedroom, living room, toilet, and kitchen. These spaces and conceptions created by very simple processes of technology create specific ideas of privacy.”

“Two common ways of understanding privacy are through secrecy and anonymity. We believe that our bank balance must be private. Companies do not normally make public the salaries of all their employees. Universities do not make public the marks or grades of their students in a way that violates the privacy of the student.”

“These notions of privacy are based on the need for security and protection. We do not want to divulge certain things about our wealth or life practices since they may be used by others to potentially harm us. So privacy becomes a way of protecting individuals or groups. But we also often overthrow privacy arguments for security purposes. We do not object to giving our biometrics when we apply for visas or when we join some private jobs.”

“Contemporary technology has made possible many innovations that have changed the very meaning and significance of privacy. From smartphones to the darknet, the fundamental trajectory is one to do with privacy. However, there are two worrisome aspects. In any discussion on privacy, there is a deep suspicion of the government and state, most times rightly so. But this suspicion does not extend to technology and its private agents, those that are responsible for the breakdown of the value of privacy today”

“Today, in times of growing privatization, the greatest challenge to privacy comes from the private sector. It also stems from indifference to our privacy. We do not seem to value privacy today as in earlier times. Social experiments have shown that people are willing to have private information about them made public if they receive some monetary advantages

We do this all the time.” When we search for a book or a ticket, we start getting advertisements related to these searches in our supposedly private emails. What we read, search, buy, talk and perhaps even think, gets stored, used, and circulated. Everything is tracked and rerouted. We have no clue to the amount of information about our private lives that are out in the Web. All because we get free emails and free Internet access! Today, privacy has been deeply compromised through the offering of ‘free’ goods.

The State and private players

“Very often when we worry about questions of privacy, it is about the role of the government or the state. The state too can do much with the information on individuals that it collects through various voluntary as well as coercive means. The concern about privacy thus was a concern about the potential misuse of such information. However, information about individuals is arguably much more in the private domain today than it is within various governments. Moreover, the mining of this information is taken up far more assiduously by the private compared to government institutions.”

“The idea of privacy has always had a troubled relationship with privatisation. Private companies often have rules that protect them from being transparent in hiring policies, in affirmative action, or even making public the salaries of all their employees. Private groups know best the power of the idea of privacy. They use this notion to protect themselves from governments and the public. They also realise that the greatest market that is perennially available to them is the market of trading information on privacy.”

“A related problem is that the government has begun to look more and more like the private sector. Today, almost all politicians are rich entrepreneurs and hold powerful business interests. The public-private binary does not function in any useful sense as far as the governing class is concerned. Thus, privacy is not only open to manipulation by the government but even more so by the private sector. This is so especially because it is the private sector that is at the forefront of developing technologies that facilitate this mining, storing, and sharing of information.”

“The Trojan horse through which the state and private players enter our domains of privacy is through contemporary technologies. These technologies have now come to be seen as necessary. The fact that we so unthinkingly buy into this story shows the success of how these technologies have colonised us so effectively.”

“The price we pay for modern technologies is not only money. The economic model that runs consumerism of modern technologies is quite different from the model of selling groceries. We are seduced by the number of free things we get in a technological gadget. The websites are free; we can download millions of books and songs for which we had to pay earlier. Why are we being given so much that is free? Like almost everything else in this world, there are always hidden costs. The major cost that we pay is the cost of our privacy — the information on each one of our private lives and, through this information, more effective control on how we act and behave.”

“This raises deeply troubling questions about making privacy a fundamental right. How will the Supreme Court judges be able to give a judgment on privacy as a fundamental right without also making possession, and the making, of technology as ‘rights’? How can they do this without imposing controls on predator technologies that enter the social world in the guise of making our lives comfortable? Some might argue that technology is only an intermediary tool that enables certain things, both good and bad.”

“But to hold this view is to be blind to the changing modes of technological domination through digital and Internet technologies. Technology is no longer outside human and social processes; it co-creates and co-constitutes the human and the social.”

3.2. Concept of Privacy

The expression "privacy" is utilized regularly in the common language just as in philosophical, political, and lawful conversations and legal discussion, yet there is no single definition or investigation or importance of the term in a

broader picture. The idea of privacy and protection of privacy has wide recorded roots in sociological and anthropological conversations about how broadly it is esteemed and saved and preserved in different societies. Additionally, the idea has chronicled origin in notable philosophical conversations, most outstandingly Aristotle's differentiation between the open circle of political movement and the private circle related to family and household life. However authentic utilization of the term isn't uniform, and there remains disarray over the significance, worth, and extent of the idea and the concept of privacy.¹⁹

At present, privacy is a general idea, incorporating (in addition to other things) opportunity of thought, authority over one's body, isolation in one's home, command over data about oneself, opportunity from observation, assurance of one's notoriety, and insurance from searches and cross-examinations. Consistently savants, legal theorist, and law specialists and jurists have regretted the extraordinary trouble in arriving at a fantastic origination of protection. Arthur Miller has announced that security is “*difficult to define because it is exasperatingly vague and evanescent.*”²⁰

*“Privacy is the ability of an individual or group to seclude themselves, or information about themselves, and thereby express themselves selectively. The boundaries and content of what is considered private differ among cultures and individuals but share common themes. When something is private to a person, it usually means that something is inherently special or sensitive to them. The domain of privacy partially overlaps security (confidentiality), which can include the concepts of appropriate use, as well as protection of information. Privacy may also take the form of bodily integrity.”*²¹

The right not to be exposed to unsanctioned intrusion of privacy by the administration that is to say the government enterprises or people is a piece of numerous nations ‘privacy laws, and now and again, constitutions. Practically all nations have laws which here and there limit security. A case of this would

¹⁹ Privacy, Stanford Encyclopaedia of Philosophy, <http://plato.stanford.edu/entries/privacy>. (visited on Feb 20, 2018).

²⁰ Daniel J. Solove, *Conceptualizing Privacy*, California Law Review, Vol. 90, No. 4 (2002), Available at: <http://www.jstor.org/stable/3481326?origin=JSTOR-pdf>. (visited on Feb 20, 2018).

²¹ *Supra* note 19

be law concerning tax assessment, which ordinarily requires the sharing of data about close to home pay or profit. In certain nations individual privacy may struggle with the right to speak freely of certain laws and a few laws may require open divulgence and full public disclosure of data which would be viewed as private in different nations and societies.

“Privacy could also be voluntarily sacrificed, normally in exchange for perceived benefits and often with specific dangers and losses, although this is often a strategic view of human relationships. For example, people could also be able to reveal their name if that permits them to market trust by others and thus build meaningful social relations. Research shows that folks are more willing to voluntarily sacrifice privacy if the info. gatherer is seen to be transparent on what information is gathered and the way it's used. In the business world, an individual may volunteer personal details (often for advertising purposes) to gamble on winning a prize. A person can also disclose personal information as a part of being an executive for a publicly-traded company within the USA pursuant to federal law. Personal information which is voluntarily shared but subsequently stolen or misused can cause fraud.”

“The concept of universal individual privacy is a modern construct primarily associated with Western culture, British and North American in particular, and remained virtually unknown in some cultures until recent times. According to some researchers, this concept sets Anglo-American culture apart even from Western European cultures such as French or Italian. Most cultures, however, recognize the ability of individuals to withhold certain parts of their personal information from wider society—closing the door to one's home, for example.”

The distinction or overlap between secrecy and privacy is ontologically subtle, which is why the word “privacy” is an example of an untranslatable lexeme, and many languages do not have a specific word for “privacy”. The distinction hinges on the discreteness of interests of parties (persons or groups), which can have emic variation depending on cultural mores of individualism, collectivism, and the negotiation between individual and group rights. The

difference is sometimes expressed humorously as “when I withhold information, it is privacy; when you withhold information, it is secrecy.”

A broad multicultural literary tradition going to the beginnings of recorded history discusses the concept of privacy. One way of categorizing all concepts of privacy is by considering all discussions as one of these concepts:

1. the right to be let alone
2. the option to limit the access others have to one's personal information
3. secrecy, or the option to conceal any information from others
4. control over others' use of information about oneself
5. states of privacy
6. personhood and autonomy
7. self-identity and personal growth
8. protection of intimate relationships

3.3. Need for privacy

1. Exercise the Limit on Power

“Privacy is a limit on government power, as well as the power of private sector companies. The more a person knows about us, the more power he or she can have over us. Vital decisions in our lives are made using personal data. It can be used to influence our position in society; and it can be used to impact our decisions and mould our behaviour. It can be used as a tool to exercise control over us. And in the hands of a malicious mind, personal data can cause great harm to us.”

2. Respect for Individuals beings

“Privacy is about respecting individuals. If someone is having a valid reason to keep something private, it is offensive to not pay attention to that person’s wishes without an appropriate reason to do so. Of course, the aspiration for

privacy can cause clashes with essential values, so privacy may not always win out in the balance. Sometimes people's desires for privacy are rendered unimportant because of the view that the harm in doing so is minor. Even if this doesn't cause severe injury, it shows a lack of respect for that person. In a sense, it is saying: "I care about my interests, but I don't care about yours."

3. Reputation Management and protection

"Privacy enables people to manage their self-esteem. Our relations, chances are given to us and overall well-being is affected by how others judge us. Shielding reputation depends on protecting against not only inaccuracy but also certain truths or knowing personal details about others. People judge badly, they judge in haste, they judge out of context, they judge without listening to the full story and they judge with hypocrisy. Privacy can lend a hand to people from getting into such exasperating and troublesome judgments."

4. Maintaining and creating Appropriate Social Boundaries

"People tend to make boundaries from others in society, which are both physical and informational. We need places of solitude to retreat to, places where we are free of other's gaze to get our peace. To make ourselves at ease. We make informational boundaries for the varied relationships we have. Privacy helps in the management of these boundaries. Negligence towards these boundaries can lead to awkward social situations and damage our relationships. Privacy reduces social friction. People don't want others to know everything about them or want to know everything about others; hence phrases "none of your business" and "too much information" came in being."

5. Trust

"In relationships, be it personal, professional, governmental, or commercial, we all depend on mutual trust. Breaches of confidentiality are breaches of trust. In professional relationships, this trust is key to maintaining candour in the relationship. We trust other people we interact with as well as do business

within the same way. If the trust is broken in one relationship it acts as a hindrance for us to trust in another relationship.”

6. Control over one’s life

Personal data affects nearly everything we can think of. It is essential to so many decisions made about us like, “Will our loan be sanctioned or not?” or “Will we get our dream job?”. It determines whether we have been involved in illegal activities, been searched at the airport, or been enquired by the government. Without knowing how our data is being used, we cannot correct it or to object when this data usage causes us harm, and in turn, makes us helpless. We cannot have autonomy and control over our own lives if so many decisions about us are being taken without our participation and awareness.

7. Freedom of Thought, speech, and expression

“The key to freedom of thought is privacy is. A watchful eye over everything that one reads or watches can push us from discovering ideas outside the mainstream. It is also the key to protect speaking unpopular messages. And privacy doesn’t just provide a shield from fringe activities. We may want to censure people we know to others yet not share that criticism with everyone. A person might want to discover ideas that their family or friends or colleagues don’t like.”

8. Freedom of Social and Political Activities

“Privacy provides shield to our ability to relate with others and engage in politics. A major component of freedom of political association is the capacity to do so with privacy if one selects. We protect privacy at the ballot because of the concern that failing to do so would chill people’s voting their true conscience. Privacy of the associations and activities that lead up to going to the voting booth is important due to the fact that is how we form and discuss our political beliefs. The watchful eye can disrupt and unduly affect these activities.”

9. Ability to Change and Have Second Chances

“Many of us are not static; we change and develop throughout our lives. Great value lies in the ability to have another chance, to be able to move further on a mistake, to be able to reinvent oneself. This ability is nurtured by privacy. It permits us to grow and mature without being shackled with all the mindless things we might have done before. Certainly, not all misdeeds should be protected, but some should be because we want to cheer up and facilitate growth and improvement.”

10. Not Having To Explain or Justify Oneself

“One of the major reasons why privacy matters are not having to explain or justify oneself. One may do a lot of things and activities, if judged from afar by others having zero knowledge or understanding, may seem odd or embarrassing or worse. It can be a heavy burden if we continuously have to imagine how everything we do will be understood by others and have to be at the ready to explain.”

3.4. Privacy as a Trade-off

It is often misconstrued that the only martyr of national surveillance is personal privacy. This is largely true, however, the impacts of personal privacy (or the lack of it) on consumer behaviour remains to be largely undocumented. A hit to privacy may have widespread economic consequences to the government as well as for-profit organisations. This phenomenon manifested itself on 6 October 2015 at the European Court of Justice.

The Safe Harbour Privacy Principles were intended to prevent private companies in the European Union or the United States from accidentally leaking private customer data stored in their systems. In a verdict²² in July 2000, the European Commission(EC) decided that US companies which adhere to seven principles and register that they meet the “safe harbour

²² Maximillian Schrems v Data Protection Commissioner, C-362/14

scheme” (a series of self-certifications), were allowed to move customer data from the EU to the US. This is referred to as the Safe Harbour decision.²³

This decision was quashed by the European Court of Justice, stating *"legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life"*

The decision, though made in the aftermath of revelations by former CIA employee and contractor Edward Snowden, has a much larger impact on businesses not just in the US but across the world. Organizations are now keener to understand the impact of the latest privacy protection laws in states and what they can do to actively comply as well as go farther to boost consumer confidence without compromising the revenues. In this case, the loss of trust of the European consumer in US companies has the potential to hurt their bottom-line in the long haul. It is now imperative for businesses to assess privacy protection, benefits from data sharing, pecuniary interests, and national security as four important pillars of consumer satisfaction and balance them in the best way possible.

Individuals sub-consciously evaluate the trade-offs between the public and private status of their data. Companies, the legal system as well as the government need to quantify the economic worth that people assign to the security of personal data.

It is imperative to organizations because depending on customers’ value assigned to privacy, managers can evaluate positive or adverse reactions at each step.

Ever-increasing global concerns over privacy have now given businesses a compelling reason to include it in their broader business strategies. Even so, organisations are fully aware that not using consumer data for targeted marketing campaigns can put them in a severe competitive disadvantage. Often the privacy guidelines recommended by the state are cost intensive and

²³ Court of Justice of the European Union, PRESS RELEASE No 117/15, Luxembourg, Oct.6, 2015

businesses resort to providing the bare minimum levels of privacy protection guided by the competition. For instance, for European firms, these are mainly based on taking customers' consent as mandated by the General Data Protection Regulation (GDPR) Such lackadaisical approach of businesses is a result of a widespread assumption that however strong the consumers' concerns over piracy, their purchasing behaviour seldom reflects these concerns.

However, a survey conducted by CISCO in 2019 has indicated that such a strategy may be myopic at best. This survey, with 2601 respondents revealed that about a third of consumers concerned about privacy are either willing to or already have changed brand loyalties as a result of the privacy protection policies of the respective firms. This group is called privacy actives and the remaining is called privacy non-actives.

The single biggest takeaway from the CISCO survey is how the privacy actives and privacy non-actives react to opportunities of trade-offs between benefits of data sharing and privacy of personal data. To the surprise of many, privacy actives were more likely to share data in lieu of benefits. More than 3/5th were comfortable with providing their buying records for customized services, compared to only 30% of non-actives. Several other trade-offs later it was established that privacy actives were roughly twice as likely to be comfortable to trade-offs as compared to non-actives. Although counterintuitive, it is clear from the study that the more privacy conscious or informed the consumers are, the more likely they are to understand the benefits of sharing data. This conclusion also finds resonance in Alessandro Acquisti's paper "Privacy in Electronic Commerce and the Economics of Immediate Gratification, 2004"²⁴ where he explains further using mathematical modelling and using the concept of marginal utility.

Businesses and policy makers can use this understanding to balance the privacy standards and the benefits accrued from sharing of data.

²⁴ Alessandro Acquisti, *Privacy in Electronic Commerce and the Economics of Immediate Gratification* H. John Heinz III School of Public Policy and Management, Carnegie Mellon University
acquisti@andrew.cmu.edu

For businesses, the starting point can be reaching out to their customers and find out their opinion on the sufficiency or insufficiency of privacy measures taken by the firm. Overtures like these can help start discussions regarding fair rewards for the use of their data.

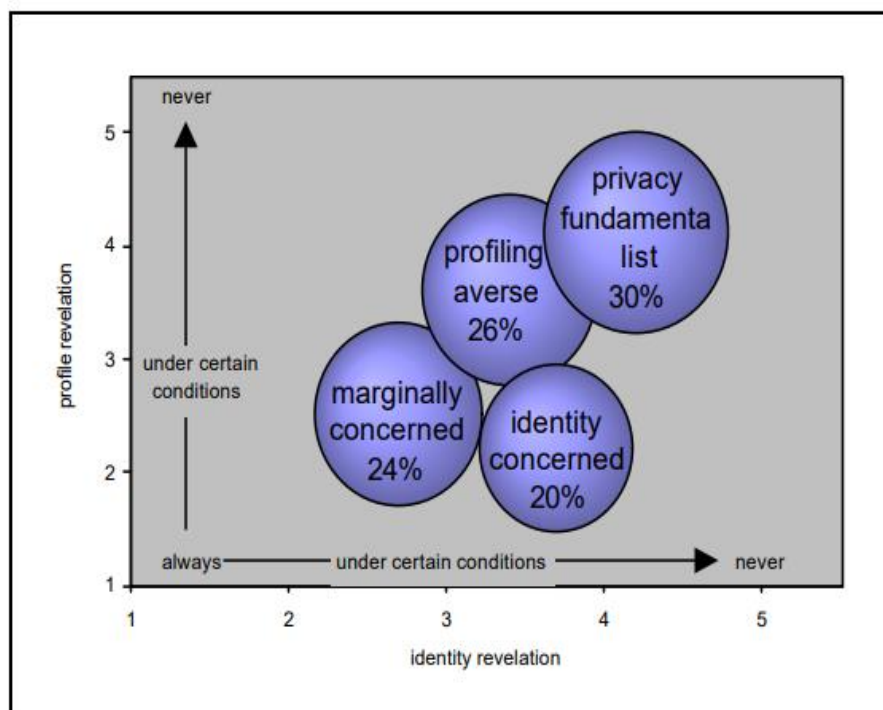
Rather than clamping down on firms by using austere rules on piracy, policy makers can address the issue of information asymmetry and bounded rationality faced by the consumers when faced with privacy challenges. According to the survey, most consumers complain that they do not know what the company is doing with their data. For instance, only 11% of users understand the purpose or meaning of cookies and the benefits or consequences of opting out or opting in, only less than half understood that cookies give away the geographic location of the computer. The role of the policy maker is to educate the consumers on privacy challenges, understanding disclosures, and trade-offs, so that they can make more informed decisions based on their privacy expectations.

Table 3: Responses to factual questions about cookies — correct answers in bold

Description	True	False	Unsure
Cookies are small bits of data stored on my computer	91%	1%	8%
Cookies let me stay logged in over time without needing to enter my password every time I visit a site	77%	8%	15%
Cookies enable personalized advertising based on my prior behavior online	76%	5%	19%
Advertisers can use cookies on multiple websites to learn which sites I visit	74%	5%	21%
Cookies may be combined with other data that identifies me by name	53%	11%	37%
If I do not accept cookies, websites cannot tell where I am physically located	12%	51%	37%
Cookies enable personalized content like color schemes or what type of information I want to see on a website	51%	14%	35%
Cookies contain information from when I first purchased my computer, including my name and home address	13%	48%	39%
Cookies let web browsers' forward and backward arrows work correctly	19%	44%	38%
Cookies are a type of spyware	39%	33%	28%
A website I visit can read every cookie I have, no matter which website the cookie is from	19%	34%	47%
Cookies let people send me spam	38%	29%	33%
Cookies change the color of hyperlinks to websites I have already visited	43%	25%	32%
Cookies let websites display more quickly	60%	19%	22%
By law, cookies may not contain credit card information	30%	11%	59%
The PATRIOT ACT allows law enforcement officials to read my cookies if I exchange email with someone on the terrorist watch list	38%	6%	56%

On a broader level, the state needs to find a justified valuation of individual privacy when trade-offs are made for *benefits*. The first attempt towards this goal was made by the 104th United States Congress in the form of Health Insurance Portability and Accountability Act of 1996 (HIPAA) signed by President Bill Clinton. Enacted with the motive of protecting personally identifiable information from theft and fraud, the act essentially traded off privacy protections for increased administrative costs. Now, in order to understand the worth of this trade-off to the patients, it is essential to quantify their individual privacy valuations. Multiple researchers have forayed into answering this puzzle in diverse contexts. We will discuss some of them here.

A study by researchers at Humboldt University Berlin reveals a disjunction between the privacy preferences as stated by the consumers and their actual behaviour in market conditions. It appears to support our inference from the CISCO survey that even the most privacy-conscious individuals are likely to trade off private information for their choice of benefits.



The study employs standard multivariate clustering techniques (k-means), to categorise subjects into four groups with different privacy-attitudes: Privacy

fundamentalists (highly privacy conscious subjects), marginally concerned users, pragmatic users (further subdivided into identity concerned and profile concerned). The identity concerns being talked about here are name, address, or/and e-mail, while profile concerns are interests, hobbies, health, and related personal data.

The results of the study are useful to understand the privacy discourse as it has proceeded in the IT age. It is one of the first of its kind to provide empirical evidence of consumers' actions regarding sensitive data. It renders a major assumption hitherto taken as a fact baseless: that privacy attitudes are directly proportional to privacy behaviours. It is in fact, quite the opposite. It calls for a change in the formation of privacy regulations: the design needs to protect individuals from different degrees of self-exposure.

When seen from the economic viewpoint, the focus of privacy research concluded so far focuses on privacy as simply protection of personal information. Such protection or concealment is assumed to be intentional and rational. In a free market, however the individuals can decide to share an optimal amount of personal information, varying with each individual. The cost of private information is subjective for each individual. When the monetary costs of information leak or sharing are quantifiable it still leads to some uncertainty in the risk (or lack of risk) of such a cost. Precise calculation of privacy valuations can also be attempted using concepts from behavioural economics and decision sciences. It is also important to consider the irrational factors that affect the decision making. In the end the consumers face two broad categories of choices when it comes to privacy challenges: benefits in lieu of personal information or cost in lieu of protecting their personal information.

Studies have focussed on the willingness to accept (WTA) versus willingness to pay (WTP)

WTA is the minimum price a consumer would accept to share personal information while WTP is the highest price a consumer would spend to buy information. WTA tends to be higher, best explained by the risk aversion of consumers. From the consideration of privacy, this difference between WTA

and WTP can predict how willing a person would be to share personal information if he has until now *not* had his personal information shared anywhere and has now been asked to pay to continue to secure his privacy. On the other hand, would someone be willing to share information for monetary benefits would reconsider his decision if this results in loss of privacy. However, the mathematical models have not been able to quantify how much consumers would be willing to spend to protect the data and/or the value they would be willing to accept to share the same. If there is a difference in the two values then it would not be possible to accurately establish the value assigned to the protection and/or sell personal information.

3.3 State Power

We discussed the economic aspects, now let us understand state affairs. In the lines of Lord Acton, “*Power corrupts and absolute power corrupts absolutely*”²⁵, with the following view this paper deals with the intricacies of the country and country’s need to hold on to the idea of constitutionalism through limited government. The Concept is then discussed about the role which the judiciary plays in protecting the rights of the citizens of the country. The paper focuses on the fundamental right of right to privacy under “*Article 21*”²⁶ of the constitution.

The question arises that what exactly is a limited government and what is the provision which deals in the privacy issues and if at all, then how can judiciary help in bridging the current situation and for harmonization between both; the government and the citizens of the country, so that neither the fundamental right under the constitution relating to privacy is curbed while also taking appropriate but not extravagant measures to keep a check on the security of the nation nor the unsolicited surveillance that happens at every digital footprint an individual leaves.

3.5.1. Genesis

²⁵ letter lord Acton wrote to scholar and ecclesiastic Mandell Creighton, dated April 1887

²⁶ INDIA CONST. Art 21.

To understand the concept of the aforesaid mentioned terms such as “constitutionalism”, “limited government”, “right to privacy”, we must first understand what is the constitution, from where it all started, and the genesis of the concepts like government, rights, etc. How the rule of law plays and important role in upholding the constitutionalism and what are the case laws which helped in developing the right to privacy as we know today.

3.6. Constitution and Definition of Constitution

In simple terms, *“The organic and fundamental law of a nation or state, which may be written or unwritten, establishing the character and conception of its government, laying the basic principles to which its internal life is to be conformed, organizing the government, and regulating, distributing, and limiting the functions of its different departments, and prescribing the extent and manner of the exercise of sovereign powers. In a more general sense, any fundamental or important law or edict”*²⁷

It can be understood from the mentioned text that the constitution is the law of the land and the supreme power vests with the constitution and the division of power amongst the three organs of the state will be based on the provisions mentioned in it or according to the constitutional conventions. Ideally, there should be a separation of power on both personnel as well as the functional level to prevent any kind of arbitrariness from any of the three organs.

*“The legislative department shall never exercise the executive and judicial powers, or either of them: the executive shall never exercise the legislative and judicial powers, or either of them: the judicial shall never exercise the legislative and executive powers, or either of them: to the end it may be a government of laws and not of men.”*²⁸

To maintain this, there should always be a system of checks and balances where each organ can stop the other from encroaching the jurisdiction of one another and formulation and execution of law is on the basis of the concept of

²⁷ Black Law’s Dictionary (9th Ed. 2009)

²⁸ Massachusetts Declaration of rights, Art 30,

“rule of law”²⁹, which is nothing but the principles against arbitrary nature of the superior authority. Rule of law is nothing but, “*Doctrine of Political Morality*” and states that balance between rights and power and between the individuals and the state should always be maintained. But, seldom has it happened that while making the legislation or while implementing them, the legislature and the executive body go out of their scope of power and formulate such laws which are arbitrary in nature and which violates curbs or abrogates the basic fundamental rights of the citizens.

3.7. Importance of Rule of Law in Maintaining Constitutionalism

Whenever the discussion about the scope of the government to make such laws takes place, it is inevitable for the discussion to shift to the scope, application and position of rule of law in that particular country. The concept of rule of law is the basic feature of constitutionalism. It is a dynamic concept. It is also a central feature of constitution system and basic feature of the constitution. The entire concept is based on, “Principle of law and not of men”. Over the years the supreme court of India has developed some principles of rule of law and thereby developing the constitutionalism. The best example of the same is given in the case of “*Veena Seth v. State of Bihar, in which the Supreme Court extended the rule of law to the poor and down trodden*”³⁰, the illiterate masses of the nation and further went on to describe that how in India no action can be taken except under the authority of law and duty has been cast upon the judges to enforce the rule of law, because even though India as a country has active rule of law in the letter as well as the spirit and it is expected that constitutionalism is natural corollary to governance in India, but, in experience last 60 years process of governance is a mixed one. Even after having an excellent administrative structure for maximum welfare, the excessive bureaucratization eventually leads to the alienation of the rulers from the ruled. It is important that the laws made must be in concurrence with the law of the land and should give equal protection of law and maintain equality before law. The downtrodden and poor people make bulk of humanity in India and the rule of law does not merely exist for people in power or who are well off and have

²⁹ John M. Gest, “THE WRITINGS OF SIR EDWARD COKE”, 18 Yale L.J. 523, 504-532 (1909).

³⁰ *Veena Seth v. State of Bihar*, A.I.R 1983 SC 339

means to fight for their rights but also for people who do not have the means, without being under the influence of the government or with excessive interference from the government.

3.8. Limited Government: Origin and Scope

Whenever the power of the government, to intervene in the lives and activities of the people is limited by the constitutional law, that kind of government is said to be a “*limited government*”. Limited government refers to any government in which its powers over the people are limited by the constitution of that country whether written or unwritten or overriding rule of law.

The basic concept is to stop “absolutism”³¹ and concentration of power which are bestowed in the hands of a single person, such as monarchs or dictators or similar sovereign.

“*Magna Carta*”³² was the first ever charter which was legally binding and was formed to limit the powers of the rulers and introduced the concept of limited government for the first time

The limited government is almost exactly opposite of the doctrine of absolutism. The ideology behind both of them is completely different. It is against the Divine Right of Kings, which grant an unlimited sovereignty to a single person over the people.

The history of limited government dates back to 1215, when Magna Carta was first introduced in the western civilization. It was not a conclusive and well defined charter and although it did limit powers of the king, it was only a small section of English people which could benefit from it but because of this development, it granted the king’s barons certain rights which were limited in nature but could be applied in opposition to the king’s policies.

After the charter of Magna Carta, other such revolutions broke resulting in other similar documents which then lead to the strengthening of the concept of

³¹ King Louis XIV (1643–1715) of France furnished the most familiar assertion of **absolutism** when he said, “L’état, c’est moi

³² King John of England (r. 1199–1216) introduced it as a practical solution to the political crisis he faced in 1215, Magna Carta established for the first time the principle that everybody, including the king, was subject to the law.

the limited government. One such example is “*The English Bill of Rights*”³³, arising from the “*Glorious Revolution*”³⁴ of 1688, which further limited the powers of the royal sovereignty. The U.S. Constitution, In contrast to the Magna Carta and English Bill of Rights, establishes a central government, which is then limited by the constitution itself along with its amendments; the government is limited by the document itself by the system of three branches of government which put limits over each

Other’s powers and the process is called the system of checks and balances. This entire process is called the “*Separation of power*”

One of the greatest accomplishments of humanity is the Limited Government ,however just a part of mankind is getting a chance to enjoy it and that too they are enjoying it imperfectly; and where so ever it is enjoyed; its tenure is ever hazardously prone to fall or crumple or is unstable. The experience of the past century has made clear the insecurity of constitutional government and the need for courage in achieving it and vigilance in maintaining it.

The people advocating the phenomenon of limited government are not Anti-Government as some people claim them to be. Rather they are only belligerent to concentrations of coercive power and to the arbitrary use of power against right. With a deep appreciation for the lessons of history and the dangers of unconstrained government, they advocate for constitutionally limited government, with the delegated authority and means to protect the rights, but not so powerful as to destroy or negate them.

The Indian legal system was established to provide limited government. The intention of the constitution framers was that the independent existence of India was based on certain truths for example that “*All Men are made equal*”³⁵, that they are bestowed by their Creator with certain unalienable

³³ Act signed into law in 1689 by William III and Mary II, who became co-rulers in England after the overthrow of King James II. The bill outlined specific constitutional and civil rights and ultimately gave Parliament power over the monarchy.

³⁴ Glorious Revolution (1688-1689) established the supremacy of parliament over the British monarch. It involved the overthrow of the Catholic king James II, who was replaced by his Protestant daughter Mary

³⁵ Thomas Jefferson , 1776 , beginning of the American Revolution coined the phrase in the original draft of declaration of independence

Rights, that among these are “*Life, Liberty, and the Pursuit of Happiness*”³⁶ is there and That to secure these Rights, Governments are established among Men, getting their equitable Powers from the Consent of the Governed, that at whatever point any Form of Government ends up ruinous of these Ends, it is the Right of the People to modify or to abrogate it, and to initiate new Government, establishing its Framework on such Principles, and sorting out its Powers in such Form, as to them will appear to be well on the way to impact their Safety and Happiness.

Masterminds of a welfare society didn't cull those certainties out of anywhere, nor did they just design the standards of the Indian government. They drew on their insight into a large number of long stretches of mankind's history, during which numerous people groups battled for freedom and limited government. There were both defeats and victories along the way.

“Through the study of history, the Founders learned about the division of power among judicial, legislative, and executive branches; about federalism; about checks and balances among divided powers; about redress and representation; and about the right of resistance, made effective by the legal right to bear arms, an ancient right of free persons. Liberty and limited government were not invented in 1947 they were reaffirmed and strengthened.” It is important to understand these concepts to determine, exactly how much of encroachment on a right can take place, the legality of it, whether the state has unfettered power or not and whether the acts of the government in terms of violating the privacy of individuals is a black spot on the system of checks and balances and what role can judiciary play, if any, to work as an effective deterrent towards the unsolicited usage of power. For further understanding, it is important to understand the legal framework of the state and how the judiciary, over time has triumphed out as the ultimate advocate of peoples rights and privacy.

³⁶ United States Declaration of Independence (1948)

CHAPTER 4

LEGAL FRAMEWORK

Richard B. Parker writes:

*“Privacy is control over when and by whom the various parts of us can be sensed by others. By sense, is meant simply seen, heard, touched, smelled, or tasted. By parts of us, is meant the part of our bodies, our voices, and the products of our bodies. Parts of us also include objects very closely associated with us. By closely associated is meant primarily what is spatially associated. The objects which are parts of us are objects we usually keep with us or locked up in a place accessible only to us.”*³⁷

4.1. Right to Privacy

“Privacy uses the theory of natural rights and generally responds to new information and communication technologies. In the United States, an article in the December 15, 1890 issue of the Harvard Law Review, written by attorney Samuel D. Warren and future U.S. Supreme Court Justice, Louis Brandeis, entitled The Right to Privacy, is often cited as the first implicit declaration of a U.S. right to privacy. Warren and Brandeis wrote that privacy is the right to be let alone and focused on protecting individuals. This approach was a response to recent technological developments of the time, such as photography, and sensationalist journalism, also known as yellow journalism”.

Privacy rights are inherently intertwined with information technology. In his widely cited dissenting opinion in *Olmstead vs. United States* (1928), Brandeis relied on thoughts he developed in his 1890 article -The Right to Privacy. But in his dissent, he now changed the focus whereby he urged making personal privacy matters more relevant to constitutional law, going so far as saying “*the government was identified as a potential privacy invader.*” He writes, “*Discovery and invention have made it possible for the Government, by means far more effective than stretching upon the rack, to obtain disclosure in court*

³⁷ Richard B. Parker, “A Definition of Privacy,”.

of what is whispered in the closet.”³⁸ At that time, telephones were often community assets, with shared party lines and the potentially nosy human operators. By the time of Katz, in 1967, telephones had become personal devices with lines not shared across homes and switching was electro-mechanical. In the 1970s, new computing and recording technologies began to raise privacy concerns, resulting in the Fair Information Practice Principles.

Alan Westin believes that new technologies alter the balance between privacy and disclosure and that privacy rights may limit government surveillance to protect democratic processes. Westin defines privacy as, “*the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others*”³⁹. Westin describes four states of privacy: solitude, intimacy, anonymity, reserve. These states must balance participation against norms:

Each individual is continually engaged in a personal adjustment process in which he balances the desire for privacy with the desire for disclosure and communication of himself to others, in light of the environmental conditions and social norms set by the society in which he lives.

Under liberal democratic systems, privacy creates a space separate from political life, and allows personal autonomy, while ensuring democratic freedoms of association and expression.

David Flaherty believes networked computer databases pose threats to privacy. He develops 'data protection' as an aspect of privacy, which involves “*the collection, use, and dissemination of personal information*”. This concept forms the foundation for fair information practices used by governments globally. Flaherty forwards an idea of privacy as information control, “*individuals want to be left alone and to exercise some control over how information about them is used*”.

Marc Rotenberg has described the modern right to privacy as Fair Information Practices, “*the rights and responsibilities associated with the collection and*

³⁸ *Ibid.*

³⁹ Merri Beth Lavagnino, *Information Privacy Revealed*, EDUCAUSE REVIEW, Jan 28, 2013 <https://er.educause.edu/articles/2013/1/information-privacy>

use of personal information". Rotenberg emphasizes that the allocation of rights is to the data subject and the responsibilities are assigned to the data collectors because of the transfer of the data and the asymmetry of information concerning data practices.

Richard Posner and Lawrence Lessig focus on the economic aspects of personal information control. Posner criticizes privacy for concealing information, which reduces market efficiency. For Posner, employment is selling oneself in the labour market, which he believes is like selling a product. Any 'defect' in the 'product' that is not reported is a fraud. For Lessig, privacy breaches online can be regulated through code and law. Lessig claims "*the protection of privacy would be stronger if people conceived of the right as a property right*", and that "*individuals should be able to control information about themselves*". Economic approaches to privacy make communal conceptions of privacy difficult to maintain.⁴⁰

4.2. International Perspective of Privacy Rights

The right to privacy is our right to keep a domain around us, which includes all those things that are parts of us, such as our body, home, property, thoughts, feelings, secrets, and identity. The right to privacy gives us the ability to choose which parts in this domain can be accessed by others and to control the extent, manner, and timing of the use of those parts we choose to disclose.

Privacy is a fundamental human right recognized in the "*UN Declaration of Human Rights, the International Covenant on Civil and Political Rights*"⁴¹ and in many other international and regional treaties. Privacy underpins human dignity and other key values such as freedom of association and freedom of speech. It has become one of the most important human rights issues of the modern age.

Most countries give citizens rights to privacy in their constitutions. Representative examples of this include the Constitution of Brazil, which says "*the privacy, private life, honor, and image of people are inviolable*"; the

⁴⁰ Aarushu sahu ,Evolution of Right to privacy,legal bites ,Jan 15 2018
<https://www.legalbites.in/evolution-right-privacy-india/>. (Visited on August 12, 2018).

⁴¹ Assembly resolution 2200A (XXI) of 16 December 1966

Constitution of South Africa says that “*everyone has a right to privacy*”; and the Constitution of the Republic of Korea says “the privacy of no citizen shall be infringed.” Among most countries whose constitutions do not explicitly describe privacy rights, court decisions have interpreted their constitutions to intend to give privacy rights. Nearly every country in the world recognizes a right of privacy explicitly in their Constitution. At a minimum, these provisions include rights of inviolability of the home and secrecy of communications. Most recently-written Constitutions such as South Africa's and Hungary's include specific rights to access and control one's personal information.⁴²

In the early 1970s, countries began adopting broad laws intended to protect individual privacy. Throughout the world, there is a general movement towards the adoption of comprehensive privacy laws that set a framework for protection. Most of these laws are based on the models introduced by the Organization for Economic Cooperation and Development and the Council of Europe.

In 1995, conscious both of the shortcomings of the law, and the many differences in the level of protection in each of its States, the European Union passed a Europe-wide directive which will provide citizens with a wider range of protections over abuses of their data. The directive on the “Protection of Individuals concerning the processing of personal data and the free movement of such data” sets a benchmark for national law. Each EU State must pass complementary legislation by October 1998.⁴³

The Directive also imposes an obligation on member States to ensure that the personal information relating to European citizens is covered by law when it is exported to, and processed in, countries outside Europe. This requirement has resulted in growing pressure outside Europe for the passage of privacy laws. More than forty countries now have data protection or information privacy laws. More are in the process of being enacted.

⁴²Privacy and Human Rights, *An International Survey of Privacy Laws and Practice*. <http://gilc.org/privacy/survey/intro.html>. (visited on April 27, 2018)

⁴³ *Ibid*

In many of the countries where privacy is not explicitly recognized in the Constitution, such as the United States, Ireland and India, the courts have found that right in other provisions. In many countries, international agreements that recognize privacy rights such as the International Covenant on Civil and Political Rights or the European Convention on Human Rights have been adopted into law.

Many countries have broad privacy laws outside their constitutions, including Australia's Privacy Act 1988, Argentina's Law for the Protection of Personal Data of 2000, Canada's 2000 Personal Information Protection and Electronic Documents Act, and Japan's 2003 Personal Information Protection Law.

Beyond national privacy laws, there are international privacy agreements. The United Nations Universal Declaration of Human Rights says "*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation.*" The Organization for Economic Co-operation and Development published its Privacy Guidelines in 1980. The European Union's 1995 Data Protection Directive guides privacy protection in Europe. The 2004 Privacy Framework by the Asia-Pacific Economic Cooperation is a privacy protection agreement for the members of that organization.

In the 1960s people began to consider how changes in technology were bringing changes in the concept of privacy. Vance Packard's *The Naked Society* was a popular book on privacy from that era and led discourse on privacy at that time.

4.2.1 View Points on Privacy

In the 1890s, future U.S. Supreme Court Justice Louis Brandeis articulated a concept of privacy that urged that it was the individual's "right to be left alone." Brandeis argued that privacy was the most cherished of freedoms in a democracy, and he was concerned that it should be reflected in the Constitution.

The Preamble to the Australian Privacy Charter provides that, "A free and democratic society requires respect for the autonomy of individuals, and limits

on the power of both state and private organizations to intrude on that autonomy. Privacy is a key value that underpins human dignity and other key values such as freedom of association and freedom of speech. Privacy is a basic human right and the reasonable expectation of every person.”

Alan Westin, the author of the seminal 1967 work “Privacy and Freedom,” defined privacy as the desire of people to choose freely under what circumstances and to what extent they will expose themselves, their attitude and their behaviour to others.

“According to Edward Bloustein, privacy is an interest of the human personality. It protects the inviolate personality, the individual's independence, dignity, and integrity.”

According to Ruth Gavison, there are three elements of privacy: secrecy, anonymity, and solitude. It is a state which can be lost, whether through the choice of the person in that state or the action of another person.

The Calcutt Committee in the UK said that, “nowhere have we found a wholly satisfactory statutory definition of privacy.” But the committee was satisfied that it would be possible to define it legally and adopted this definition in its first report on privacy.

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 of information.

4.2.2. United States and the Right to Privacy

“While the US constitution does not mention right to privacy explicitly, the Supreme Court has on various instances interpreted various amendments to state that the right does exist. In particular the 1974 Privacy Act was passed with the intention of protecting citizens from any federal agency using their records arbitrarily. It requires agencies to maintain an account of the disclosure of records they maintain. Further, a federal law maintains the privacy of the social security number from government inquiries, except in cases of when the status on taxes being paid has to be produced and in the case of child support.”

Eisenstadt vs. Baird and Roe vs. Wade

As the constitutional right to privacy grew, it became more awkward. In *Eisenstadt vs. Baird*⁴⁴, the Court relied on *Griswold* to invalidate a Massachusetts ban on the distribution of contraceptives to unmarried people. Over only one dissent, Justice Brennan wrote that “if the right of privacy means anything, it is the right of the individual, married or single, to be free from unwarranted governmental intrusion into matters so fundamentally affecting a person as the decision whether to bear or beget a child.” A differently inclined Justice might have written, “If the right of privacy means anything, it does not license a birth-control activist to dole out medical devices to an overflow crowd of college students.” But by the time of *Eisenstadt*, “privacy” had become a constitutional metonym, a word that resonates with the vocabulary of common experience but carries a more complicated meaning in the pages of the U.S. Reports. To be fair, the Court was hardly engaged in doublespeak.⁴⁵

The privacy right at issue was in substance the woman’s, not Baird’s, and when we speak of “private” decision making, we may mean not only that it is physically cached but that it is closed to external influence or input. The right to privacy emerges from a powerful, and powerfully American, intellectual strain. In a liberal society, an individual decision either to risk or to invite pregnancy is simply not the communities to make, and there is nothing malapropos in conceiving of that decision as grounded in a right to privacy. A difficulty arises, however, when the right has to bear the weight of justification for an exemption from abortion restrictions, as it did the following year in *Roe vs. Wade*.⁴⁶ Apart from its much-maligned trimester framework, *Roe* is not a doctrinal aberration. As Justice Brennan certainly knew, his words in *Eisenstadt* could as easily have been describing the right to obtain an abortion. The *Roe* Court’s conclusion — that “the right of personal privacy includes the abortion decision, but that this right is not unqualified and must be considered against important state interests in regulation” — was virtually unassailable as doctrine went. The problem was that the doctrine was inadequate to its broader

⁴⁴ 405 U.S. (1972).

⁴⁵ *Ibid.*

⁴⁶ 410 U.S. (1973).

task. The state's interest in preserving potential human life is spectacularly weighty, and only an equally weighty interest could counteract it in a minimally satisfying way. Framed in privacy terms, the abortion right seems not to outweigh the state's interest but to reject it altogether: asserting a constitutional right to privacy is precisely a declaration that the state may not legitimately be interested. To be private is, after all, not to be public. Extending privacy doctrine to abortion thereby abides conceiving of the decision whether to terminate a pregnancy as a zero-sum duel between state and woman, rather than as a respectful weighing of competing but equally legitimate interests.⁴⁷

Carey vs. Population Services International

The Court recognized its mistake, at least implicitly, earlier than is often thought. With the exception of *Carey vs. Population Services International*⁴⁸, which applied *Griswold* to the distribution of contraceptives to minors, the right to privacy has not been used to extend constitutional protection to previously unprotected acts since *Roe*. Feel free to reread the previous sentence, because this fact is easy to lose sight of amid the sequins and pyrotechnics of judicial confirmation hearings and talk radio. To the extent the Court has expanded the scope of substantive due process in the decades since *Roe*, it has generally done so under the auspices of "liberty," in harmony with the *Griswold* opinions of Justices Harlan and White and, as we will see in Part II, with the longstanding views of Justice Stevens.⁴⁹

Cleveland Board of Education vs. LaFleur

Thus, in *Cleveland Board of Education vs. LaFleur*⁵⁰, the Court invalidated a school board's policy of requiring unpaid maternity leave for pregnant employees, lasting from five months before their expected delivery date until three months after the child's birth. Justice Stewart, who had joined the *Roe* majority but had made clear his distaste for a constitutional right to privacy, referred in *LaFleur* to "a right to be free from unwarranted governmental

⁴⁷ *Ibid.*

⁴⁸ 431 U.S. (1977).

⁴⁹ *Ibid.*

⁵⁰ 414 U.S. (1974).

intrusion” in the “decision whether to bear or beget a child,” but he conspicuously avoided any reference to the word “privacy.”⁵¹

Moore vs. City of East Cleveland

Likewise, in *Moore vs. City of East Cleveland*⁵², the Court struck down the city’s cramped definition of “family” for the purpose of public housing eligibility. Justice Powell’s plurality opinion referenced a longstanding “freedom of personal choice in matters of marriage and family life” and “a private realm of family life which the state cannot enter” but did not rely on any right to privacy as such. If there was any doubt that the plurality was self-consciously distancing itself from the right to privacy, Justice Powell put those doubts to rest by quoting extensively from Justice Harlan’s dissent in *Poe vs. Ullman*⁵³ and concurrence in *Griswold*, both of which spoke in terms of liberty rather than privacy.

Cruzan vs. Director, Missouri Department of Health

Later, in *Cruzan vs. Director, Missouri Department of Health*⁵⁴, Chief Justice Rehnquist wrote that “the Due Process Clause protects an interest in life as well as an interest in refusing life-sustaining medical treatment.” But elsewhere in the opinion he was careful to note that “although many state courts have held that a right to refuse treatment is encompassed by a generalized constitutional right of privacy, we have never so held and believe this issue is more properly analyzed in terms of a Fourteenth Amendment liberty interest.”

Troxel vs. Granville

Again, in *Troxel vs. Granville*⁵⁵, in affirming the right of a mother to refuse visitation to her children’s paternal grandparents, Justice O’Connor grounded the Court’s decision in liberty interests and made no reference to a constitutional right to privacy.

⁵¹ *Ibid.*

⁵² 431 U.S. (1977).

⁵³ 367 U.S. (1961).

⁵⁴ 497 U.S. (1990).

⁵⁵ 530 U.S. (2000).

Bowers vs. Hardwick

Whatever might be said of cases like *Cruzan* and *Troxel*, the right to privacy had no better bellwether than *Bowers vs. Hardwick*⁵⁶. In his majority opinion rejecting *Hardwick*'s claim to constitutional protection, Justice White wrote, "We first register our disagreement with the Court of Appeals and with respondent that the Court's prior cases have construed the Constitution to confer a right of privacy that extends to homosexual sodomy and for all intents and purposes have decided this case." Although the Court of Appeals had indeed relied on the right to privacy in invalidating the statute, Laurence Tribe's Supreme Court oral argument on *Hardwick*'s behalf had made no reference to any general right to privacy.⁵⁷ Indeed, at oral argument, only Michael Hobbs, counsel for the State of Georgia, had framed the requested right in constitutional privacy terms, and he had done so at three different points in his argument. Likewise, the state's merits brief had mentioned "*the right of privacy at every available opportunity, even using the phrase as the title of a section of the brief, whereas the respondent's brief had focused much more on the inadequacy of Georgia's purported state interest. Any right invoked more enthusiastically by its enemies than its friends is not long for this Earth.*"⁵⁸

*"To say that the Court has not yet succeeded in discovering a formula that can be applied readily to any situation that may arise is only to recognize a condition of constitutional jurisprudence that is characteristic whenever important claims or interests clash. What the Court has been doing in a somewhat tentative way is to insist that privacy-dignity claims deserve to be examined with care and to be denied only when an important countervailing interest is shown to be superior."*⁵⁹

Although the Constitution does not explicitly include the right to privacy, the Supreme Court has found that the Constitution implicitly grants a right to

⁵⁶ 478 U.S. (1986).

⁵⁷ *Ibid.*

⁵⁸ *Supra* Note 57.

⁵⁹ William M. Beaney, "*The Right to Privacy and American Law*", DUKE L.J. (1965)

Available at: <https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=3107&context=lcp>. (visited on April 20, 2018).

privacy against governmental intrusion from the First Amendment, Third Amendment, Fourth Amendment, and the Fifth Amendment. This right to privacy has been the justification for decisions involving a wide range of civil liberties cases, including “*Pierce vs. Society of Sisters*”, which invalidated a successful 1922 Oregon initiative requiring compulsory public education, *Griswold vs. Connecticut*, where a right to privacy was first established explicitly, *Roe vs. Wade*, which struck down a Texas abortion law and thus restricted state powers to enforce laws against abortion, and *Lawrence vs. Texas*, which struck down a Texas sodomy law and thus eliminated state powers to enforce laws against sodomy. The 1890 Warren and Brandeis article “The Right to Privacy” is often cited as the first implicit declaration of a U.S. right to privacy. This right is frequently debated. Strict constructionists argue that such right exists (or at least that the Supreme Court has more jurisdiction to protect such a right), while some civil libertarians argue that the right invalidates many types of currently allowed acts not to be surveillance (wiretaps, public cameras film industry, etc.).

Most states of the United States also grant a right to privacy and recognize four torts based on that right:

- Intrusion upon seclusion or solitude, or into private affairs;
- Public disclosure of embarrassing private facts;
- Publicity which places a person in a false light in the public eye; and
- Appropriation of name or likeness.

“The 4 privacy torts above were introduced by William Prosser, some even argue this in addition to the right to privacy by Warren and Brandeis form the basis for modern U.S. privacy legislation. Also, in some American jurisdictions the use of a person's name as a keyword under Google's AdWords for advertising or trade purposes without the person's consent has raised certain personal privacy concerns.”

Right to privacy and social media content laws have been considered and enacted in several states, such as California’s “online erasure” law protecting minors from leaving a digital trail. However, the United States is still far behind that of European Union countries in protecting privacy online. For example, the “right to be forgotten” ruling by the EU Court of Justice protects

both adults and minors. On March 11, 2015, Intelligence Squared US, an organization that stages Oxford-style debates, held an event centered on the question, “*Should the U.S. adopt the 'Right to be Forgotten' online? The side against the motion won with a 56% majority of the voting audience.*”⁶⁰

4.3. Privacy Laws in Other Countries

4.3.1. European Union

“The Data Protection Directive adopted by the European Union in 1995 regulates the processing of personal data within the European Union. Article 8 of the ECHR⁶¹ provides a right to protection of one’s private and family life subject to certain restrictions as prescribed by law and necessary in a democratic society towards a legitimate aim. However, there is no independent tort law doctrine which recognizes a right to privacy. This has been confirmed on a number of occasions.”

Expansion of privacy law

“British Radio Jockey Sara Cox's case against The People newspaper was one of the first celebrity privacy cases. The media referred to the case as a “watershed”. The disc jockey sued after the newspaper printed nude photographs of her taken while on her honeymoon. However, the case was settled out of court and so did not establish a precedent. The decision was seen as discrediting the Press Complaints Commission.”

The expansion of the doctrine of breach of confidence under the Human Rights Act began with the “*Douglas v Hello Ltd*”.⁶² Decision. Section 6 of the Human Rights Act requires English courts to give effect to the rights in the Convention when developing the common law. There is no need to show a pre-existing relationship of confidence where private information is involved and the courts have recognized that the publication of private material represents a detriment in itself. The Human Rights act has horizontal effect in disputes between private individuals meaning that the Human Rights Act is

⁶⁰ Ananya Chakraborty, “*The U.S. Should Adopt the 'Right to Be Forgotten'*”, NEWS 18 INDIA, Aug 24, 2017, Available at: www.intelligencesquaredus.org.

⁶¹ European Convention on Human Rights, Rome, 4.XI.1950

⁶² [2005] EWCA Civ 595.

just as applicable as if one party had been a public body. Breach of confidence now extends to private information (regardless of whether it is confidential) so as to give effect to Article 8 of the European Convention on Human Rights. Before this breach of confidence afforded “umbrella protection” to both personal and non-personal information.

4.3.2. Australia

There is no statutory definition of privacy in Australia. ALRC⁶³ was given a reference to review Australian privacy law in 2006. During that review it considered the definition of privacy in 2007 in its Discussion paper. The ALRC found there is no “*precise definition of universal application*” of privacy; instead it conducted the inquiry considering the contextual use of the term “privacy”. In reaching that conclusion, the ALRC began by considering the concept of privacy:

“It has been suggested that privacy can be divided into some separate, but related concepts:

- “Information privacy, which involves the establishment of rules governing the collection and handling of personal data such as credit information, and medical and government records. It is also known as data protection”
- “Bodily privacy, which concerns the protection of people’s physical selves against invasive procedures such as genetic tests, drug testing and cavity searches”
- “Privacy of communications, which covers the security and privacy of mail, telephones, e-mail and other forms of communication.”
- “Territorial privacy, which concerns the setting of limits on intrusion into the domestic and other environments such as the workplace or public space. This includes searches, video surveillance and ID checks.”

4.3.3. Sweden

“Despite being one of the first countries of the world to give a personal identification number to its citizens, required to be used in every interaction

⁶³ The Australian Law Reform Commission

with the State, Sweden is also one of the first countries to have a detailed statute on privacy laws online. The 1973 Data Act protected the privacy of personal data on computers. The right to protection of personal data is also found in the Swedish constitution.”

4.3.4. Germany

“A horrific history of Germany under the Nazi regime, facing constant surveillance from the government, followed by persecution, has ensured that the country has emerged extremely cautious of the threat of administrative attempts at intruding into personal lives of individuals. Over time the Germans have ensured that privacy laws in the country evolved and remain updated to match with the social and technological necessities of the time. At present, it remains one of the strictest countries to enforce privacy laws and most detailed data privacy laws in the world. In the recent past in fact, the privacy law Germany has caused much discomfort to organizations like Facebook and Google which run on the basis of the freedom of the internet.” The citizens' right to protection is stated in the Constitution of Germany, in Art. 2 para. 1, and Art. 1 para. 1. The citizens' data of Germany is mainly protected under the Federal Data Protection Act (1977) from corporations, which has been amended the most recently in 2009. This act specifically targets all businesses that collect information for its use. The major regulation protects the data within the private and personal sector, and as a member of the European Union (EU), Germany has additionally ratified its act, convention, and additional protocol with the EU according to the EU Data Protection Directive 95/46 EC.⁶⁴

4.3.5. South Africa

The Constitution of South Africa guarantees the most general right to privacy for all its citizens. This provides the main protection for personal data privacy so far.

⁶⁴ *Id* at 60

The Protection of Personal Act⁶⁵ 2013 (POPI) was signed into act, focusing on data privacy and is inspired by other foreign national treaties like the United Kingdom. Minimum requirements are presented in POPI for the act of processing personal data, like the fact that the data subject must provide consent and that the data will be beneficial, and POPI will be harsher when related to cross-border international data transfers, specifically with personal information. However, POPI won't be in full effective until an estimated date of 2018 as it is still being deliberated by the National Council of Provinces.

The recording of conversations over phone and internet is not allowed without the permission of both parties with the “*Regulation of Interception of Communications and Provision of Communications Related Ac.*” (2002).

4.3.6. Canada

First brought into place in 1977 as part of the Canadian human rights act, the privacy law in Canada has evolved over time. Initially, the law was introduced as a means of data protection. In 1983, the law was expanded to include a check on how the government can access and disclose personal information. The last time the privacy law was redefined and developed was in January 2012 when the Canada government stated that the common law recognized the right to personal privacy as a “tort of intrusion upon seclusion.”⁶⁶

4.3.7. Japan

“After European Union, Japan introduced a separate central legislation for protection of data as the Act on the Protection of Personal Information (APPI). The Act took partial effect in 2016 and has been enforceable from May 30, 2017. The law defines the scope of the legislation and states on whom the law is applicable under Article 2-4 of the APPI. As per the Act, it is applicable to four entities- state institutions, local public bodies, independent administrative agencies and an entity not having over 5,000 individuals’ personal information for more than six months. Similar to the EU law, consent of a data subject forms the essence of the legislation and has been stated as mandatory in case

⁶⁵ Government Gazette Notice 37067 on 26 November 2013.

⁶⁶ Ananya Chakraborty, “*The U.S. Should Adopt the 'Right to Be Forgotten'*”, NEWS 18 INDIA, Aug 24, 2017, Available at: www.intelligencesquaredus.org.

of transmitting data to a third party or for any use beyond communication purposes. The Act on the Protection of Personal Information was fully enacted in 2005 to protect the rights and interests of individuals while taking consideration of the usefulness of personal information. The law applies to business operators that hold the personal information of 5,000 or more individuals.

4.4. Right to Privacy in India

A nine-judge bench of the Supreme Court headed by Chief Justice JS Khehar, in the case *Justice K.S. Puttaswamy and Anr. Vs. Union of India and Ors.*⁶⁷ ruled on August 24, 2017 states that the Right to Privacy should be a fundamental right for Indian citizens under the Constitution of India (under Article 21 of Part III). Therefore, no legislation passed by the government can violate it improperly. To be specific, the court selected the three-pronged test required for encroachment of any Article 21 right – legality-i.e. by an existing law; necessity, in terms of a legitimate state proportionality and objective that ensures a rational core between the means adopted to achieve that object and the object of the invasion. This clarification was important to prevent the dilution of the right in the future on the inclines and promotes the government in power. This ruling from supreme Court will open debate about the discarding of the archaic section 377, that criminalizes Homosexual acts of union. India is the world’s biggest democracy and after this ruling, it has joined Canada, United States, UK, South Africa, and the European Union where they identify this as fundamental right.

4.4.1. Historical Development in India

John Stuart in his essay “On Liberty” threw some light to the need to preserve a zone within which the liberty of the citizen would be free from the authority of the state, in 1859. In late 1890, Samuel D Warren and Louis Brandeis stated the need of right to enjoy life which included ‘right to be alone’. The right “to be let alone” therefore represented a form of “an inviolate personality”, a core of freedom and liberty from which the human being had to be free from intruders. It justifies the need of being left alone along with the early new developments in newspaper, technology, and photography.

The motive behind introducing such a principle was to protect personal productions and personal writings, not just from theft and physical appropriation but also against publication in any form which might not be consensual in nature. Therefore, at the time when technology and development

⁶⁷ AIR 2017 SC 4161.

change started threatening the individual in public viewing, many distinguished jurists referred the right to be let alone as an addition to the law of privacy.

i. Right to privacy in India before Independence

“Several researchers along with this author and academic scholars and experts have pointed out with exasperation the absence of a term in most of the popular languages in India that adequately captures all the facets of the concept of individual privacy. This is not to argue that there was no favored notion of privacy in ancient or medieval India. The point is being made that the local language variants do not include facets such as- beliefs, thoughts, correspondence, faith, the nearly inviolate privacy of one's home, as we all the necessity of protecting personal information from getting misused by public or private agencies or its commercial use without the informed consent of the person.”

ii. Constitution of India Bill, 1895

“The idea of a right to privacy as trump against the power and might of the State to interfere with personal freedoms is first expressed in the Constitution of India Bill drawn up in 1895 by authors who recognizes is not well established.” Bal Gangadhar Tilak who announced: “*Swaraj is my birth right*” and Mrs. Annie Besant who founded the Home Rule League in India are said to be the inspiring leaders behind this Bill. The text of the Bill recognized that “*Every citizen has in his house an inviolable asylum*” - a simple articulation of the classic English notion of privacy- for every man his home is his castle and the State could not invade it without lawful and legitimate justification.⁶⁸

iii. The Commonwealth of India Bill, 1925

⁶⁸ “*Evolution of Right to privacy*”, RTI Foundation of India, Aug 10, 2015.

<http://www.rtifoundationofindia.com/evolution-right-privacy-india#.WvabwIiFM2w> (visited on April 12, 2018).

“Under the Chairmanship of Sir Tej Bahadur Sapru another Bill was taken up for self-governance in India. Mahatham Gandhi, Bipan Chandra Pal and Mrs. Sarojini Naidu were members of the Committee that compiled this Bill.” This Bill identifies “Every person shall have the fundamental right to liberty of person and security of his dwelling and property.” The notion of privacy now extends to personal liberty and security for one's property apart from one's home.

iv. The Nehru (Swaraj) Report, 1928

Three years later the Indian National Congress compiled a committee under the Chairmanship of Motilal Nehru to come up with a plan for Swaraj (self-rule) for India. Eminent freedom fighter Netaji Subhash Chandra Bose was a member of this Committee. This Committee creates a negative obligation on the State vis-a-vis privacy: “No person shall be deprived of his liberty nor shall his dwelling or property be entered, sequestered or confiscated save in accordance with the law”. The multifarious aspects of the notion of privacy identified in Anglo-Saxon jurisprudence is evident in this formulation.

v. Constituent Assembly (CA) debates on the right to privacy

“The Constituent Assembly set up an Advisory Committee on Fundamental Rights, Minorities etc. chaired by Sardar Vallabhbhai Patel. A sub-Committee on Fundamental Rights was made under the Chairmanship of Acharya J B Kripalani. Various members of the CA sent their views on what fundamental rights guarantees must be incorporated in the Constitution and why.”

On the right to privacy, K T Shah wanted the following formulation (December 1946): *“Every citizen of India has and is hereby guaranteed security of his person, papers, property, house or effects against unreasonable searches or seizure.”*

K M Munshi's note quote for this formulation in March 1947:” Every citizen... has the right to the inviolability of his home. Every citizen has the right to the secrecy of his correspondence. Every person has the right to be free from interference in his family relations.” Two rights were identified for citizens and one for everybody including non-citizens.

Harnam Singh quotes this formulation inspired by the Czech Constitution (March 1947): "Every dwelling shall be inviolable". The right to privacy was expected to be attached to a physical space instead of an individual's person.

Dr. B R Ambedkar gave a more elaborate formulation (March 1947) favoring towards a collective right over an individual one: "The 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 of affirmation, and particularly describing the place to be searched and the persons or things to be seized." Dr. Ambedkar desired to fit in a strong safeguard against violation of the right to privacy along with allowing for State action where required under strict monitoring by judicial

In March 1947, the Subcommittee on Fundamental Rights approved the following draft formulation for discussion: "The right to inviolability of his home - to all persons. The right of secrecy of his correspondence - to all citizens". In late April, the final formulation was accepted and approved as follows: "The 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 of affirmation, and particularly describing the place to be searched and the persons or things to be seized. The right of every citizen to the secrecy of his correspondence." The compromise formula recognized the language proposed by Dr. Ambedkar and K T Shah and K M Munshi.

However, noted jurist Alladi Krishnaswamy Ayyar, former Editor of Hindustan Times Sardar K M Panikkar both members of the CA and its eminent constitutional advisor Benegal Narasingh Rau hampered in this work. They argued that guaranteeing the right to privacy would hinder law enforcement and the criminal prosecution of conspirators who will most likely be captured in their dwellings. They also mentioned that the Constitution of USA did not explicitly guarantee the right to privacy to its people. So, the Advisory Committee on Fundamental Rights dropped the proposal to recognize the right to privacy as a fundamental right. However, the right to

property and protection for the person of the individual were added as separate fundamental rights in Article 19 and 21. Much later the right to privacy was reduced to a constitutional right and inserted as Article 300A in the Constitution. So, the Constitution was written and then enforced in 1950 without an explicitly recognizing the individual's privacy as a fundamental right.

4.5. Data Protection Laws in India

“India’s existing laws on data privacy are much narrower in scope. The primary statutes governing data privacy are the Information Technology Act, 2000 (IT Act) and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (Privacy Rules).”

“First, Indian laws primarily regulate the processing of sensitive personal data or information (SPDI) which is a subset of personal information. SPDI includes, among other things, information relating to passwords, financial information, medical records, sexual orientation, and biometric information. Non-sensitive personal information is still subject to little regulation in India. Second, under the Indian legal framework, the requirement for consent from the individual citizen is vague enough to allow for implied consent. Further, while Indian laws do confer limited extra-territorial jurisdiction, the applicability of these laws in certain scenarios remains unclear. For instance, it is questionable whether the IT Act or the Privacy Rules would apply to a United States company that collects an Indian citizen’s/resident’s SPDI while the latter is travelling in the United States.”

“Often confused with trade secrets and confidentiality, privacy refers to the use and disclosure of personal information and is only applicable to information specific to individuals. Since personal information is a manifestation of an individual personality, the Indian courts including the Supreme Court of India, have recognized that the right to privacy is an integral part of the right to life and personal liberty, which a fundamental right is

guaranteed to every individual under the Constitution of India. As such, the right to privacy has been given paramount importance by the Indian judiciary and can only be fettered with for compelling reasons such as, security of the state and public interest.”

“Presently, there is no specific legislation with dealing with privacy and data protection. The protection of privacy and data can be derived from various laws pertaining to information technology, intellectual property, crimes and contractual relations.”

4.5.1. “Information Technology Act, 2000”

“The IT Act provides for safeguard against certain of breaches in relation to data from computer systems. The said Act contains provisions to prevent the unauthorized use of computers, computer systems and data stored therein. The section creates personal liability for illegal or unauthorized use of computers, computer systems and data stored therein. However, the said section is silent on the liability of internet service providers or network service providers, as well as entities handling data. As a result, the entities responsible for safe distribution and processing of data like the vendors and outsourcing service providers are out of the purview of this section.”

“The liability of the entities is further diluted in Section 79 by providing the criteria of knowledge and best efforts before determining the quantum of penalties. This means that the network service provider or an outsourcing service provider would not be liable for the breach of any third-party data made available by him if he proves that the offence or contravention was committed without his knowledge, or that he had exercised all due diligence to prevent the commission of such offence or contravention. It may be noted that if there is any alleged violation of the IT Act by a company, its key employees (managers and directors) are made personally liable for intentional or negligent act resulting in the violation of the IT Act.”

“The law makes no differentiation based on the intentionality of the unauthorized breach, and no criminal penalties are associated with the breach. Section 65 offers protection against intentional or knowing

destruction, alteration, or concealment of computer source code while Section 66 makes alteration or deletion or destruction of any information residing in a computer an offence. Both sections 65 and 66 are punishable with criminal penalties including imprisonment up to 3 years.”

“The IT Act is not the Act which solely deals with personal data protection. The provisions related to personal data protection has been inserted in the Act vide amendments in 2006 and 2008 in response to EU Directive and negative Press around data theft in call centers. The issue of data protection is generally governed by the contractual relationship between the parties. The parties are free to enter into agreements and determine their relationship but subject to section 43A, 72A and 69 of the IT Act.”

Section 69 is an exception to general rule of privacy and secrecy of information. It states that “the Central or State Government or any of its officer authorized by Central or State Government can intercept, monitor or decrypt any information transmitted received or stored through any computer resource in the interest of

1. Sovereignty or integrity of India,
2. Defense of India,
3. Security of the State,
4. Friendly relations with foreign States or
5. Public order or
6. Preventing incitement to the commission of any cognizable offence relating to above or
7. Investigation of any offence.”

It gives the power to the Central and State Government and agency authorized by them to access information relating to personal in nature also. The government can interfere with the data subject to recording reasons in writing.

Section 72 of IT Act states- *“Breach of confidentiality and privacy - Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuant of any of the powers conferred under this Act, rules or regulations made there under, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.”*

4.5.2. Information Technology (Reasonable Security Practices And Procedures And Sensitive Personal Data Or Information) Rules, 2011

“After European Union enacted strict and stringent Data protection laws, the Ministry of Communications and Information Technology enacted IT Rules in 2011.” “The Act contains provisions with respect to three categories- Body Incorporates, government and Information Providers. Through a Press note released in 2011 itself, the Ministry stated clearly that the rules are applicable to both the corporates and the individuals. It was framed under section 43A of IT Act after the amendment in IT Act in 2008. It gives definition of sensitive personal data.” It states that “sensitive personal data includes⁶⁹

- passwords;
- financial information, such as bank account or credit card or debit card or other payment instrument details;
- physical, physiological and mental health conditions;
- sexual orientation;
- medical records and history;
- biometric information;

⁶⁹ Rule 3 of IT Rules.

- any details relating to the above clauses as provided to a body corporate for provision of services; and
- Any information received under the above clauses by a body corporate for processing, or which has been stored or processed under lawful contract or otherwise.”

“The proviso to this definition clearly states that any information which is freely available or accessible in the public domain or under Right to Information Act, 2005 shall not be considered as sensitive personal data.” The IT Rules define personal information as “any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such a person.” No legislation provides definition of personal data except IT rules.

*“Further the IT Rules cast a duty upon the Body Corporate to provide a privacy policy which shall be available on the website of such Body Corporate.”*⁷⁰ The policy shall deal with the personal information and sensitive data including purpose of collection and its usage. *“The IT Rules moreover deal with the process and procedure that should be adopted by the Body Corporate for collection of the personal information and sensitive data.”*⁷¹

“It also states that the Body Corporate cannot retain the information longer than it is lawfully required. The Body Corporate is also required to seek the consent of the information provider before disclosing it to the third party. Exception is given to Government agencies mandated under the law to obtain information related to personal information and sensitive data. The Body Corporate has to comply with reasonable security practices as provided under Rule 8 of the IT Rules. Therefore, it can be said that the new law is stricter and stringent and in par with EU laws, the Body Corporate has duty to comply with IT Rules and ensure transparency in its new privacy policies.”

⁷⁰ Rule 4 of IT Rules.

⁷¹ Rule 5 of IT Rules.

4.5.3. Intellectual Property Rights

*“The Indian Copyright Act prescribes mandatory punishment for piracy of copyrighted matter commensurate with the gravity of the offence. Section 63B of the Indian Copyright Act provides that any person who knowingly makes use on a computer of an infringing copy of computer program shall be punishable for a minimum period of six months and a maximum of three years in prison.”*⁷² It is pertinent to mention here that the Indian courts recognize copyright in databases. “It has been held that compilation of list of clients/customers developed by a person by devoting time, money, labor and skill amounts to “literary work” wherein the author has a copyright under the Copyright Act. As such if any infringement occurs with respect to data bases, the outsourcing parent entity may have recourse under the Copyright Act also.”

4.5.4. Indian Penal Code

The Indian Criminal law does not specifically address breaches of data privacy. Under the Indian Penal Code, liability for such breaches must be inferred from related crimes. For instance, Section 403 of the India Penal Code imposes criminal penalty for dishonest misappropriation or conversion of “movable property” for one’s own use.

4.6. Industry Initiative

In India, the efforts at complying with the demands of adhering to privacy laws have originated mainly from the private sector rather than the Government. In the absence of a specific legislation, the Indian software and outsourcing industry has been taking initiatives on its own that would provide comfort to the foreign clients and vendors. The National Association of Service & Software Companies (“NASSCOM”) is India's national information technology trade group and has been the driving force behind many private sector efforts to improve data security. For example, NASSCOM has created a National Skills Registry which is a centralized database of employees of the IT

⁷² Vinita Bali , *Data Piracy: Can India Provide Adequate Protection for Electronically Transferred Data?*, SANTA CLARA LAW DIGITAL COMMONS, 21 TEMP. INT’L & COMP. L. J. 103 (2007)

services and BPO companies. This database is for verification (with independent background checks) of the human resources within the industry.

Further, a self-regulatory organization has been launched which will establish, monitor and enforce privacy and data protection standards for India's business process outsourcing ("BPO") industry. The organization has already completed its initial round of funding and the final rollout phase including industry membership is underway. Additionally, many BPO service providers in India have engaged in voluntary self-regulation and adopted stringent security measures to reduce the risks of misuse of non-public personal data. To reduce the risks of misuse of non-public personal data, the BPO companies in India have adopted one or more of the following stringent security measures:

- Posting of armed guards outside office premises.
- Restricting entry by requiring microchip-embedded swipe cards.
- Prohibiting bags and briefcases in the work area.
- Making provisions that computers in workstations have no printers or devices for removable storage.
- Banning or restricting agents or visitors from carrying mobile phones to the production floor.
- Forbidding phone calls to and from either family or friends in employee workstations.
- Disallowing image capturing devices like cell phones, scanners or photocopiers.
- Restricting or prohibiting internet and e-mail access at workstations and inside most BPO companies.
- Encryption of key information, such as passwords and, thus, unseen by employees.
- Monitoring employees via closed-circuit television.

The aforesaid protections to tighten security are an attempt by the Indian industry to ease customer concerns over theft of private information.

India, only being an off-shoring destination, the process of data collection, seeking consent of the customers/employees regarding the data, etc. is carried out in India. As such, safe harbor principles and AICPA principles may not apply on the Indian leg of the operations insomuch so that the data collection is not being done by the Indian entities. While entering into contracts, the off-shoring vendors imbibe terms and specific conditions in their contracts for data protection in line with the Graham-Leach Bliley Act, Health Insurance Portability and Accountability Act, Fair and Accurate Credit Transactions Act, etc. Typically, these vendor agreements stipulate how the information can be disclosed and provide for implementation of administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the data provided to the vendors.

With respect to the personal and financial data being misappropriated by the employees or any other persons while the data is in possession of the Indian vendors, Indian legislation recognizes copyright in database⁷³ and as such, the foreign entity may take legal action against the infringer. Since the Supreme Court of India recognizes privacy under right to life, the person whose personal data has been leaked may also take legal recourse against the alleged culprit.

The lack of a comprehensive legislation pertaining to privacy and data protection has been a matter of concern. This concern has been particularly expressed by foreign companies that are doing business in India and are transmitting confidential data into the country. Even though the data protection laws are not specifically laid down in any statute as yet, the Indian industry as well as the have begun the process of sensitizing the Government and the masses regarding the importance of privacy. Further, with regulators like the Reserve Bank of India providing for strict privacy norms in certain areas, it seems that India is taking a huge step towards privacy norms. It is being felt by all concerned that a dedicated data protection law would give further impetus

⁷³ Burlington Home Shopping Pvt. Ltd. v. Rajnish Chibber, 61,DLT 6(1995)

to not only the outsourcing industry but to the Foreign Direct Investment Policy at large.

With the changing needs and demands of the society, the laws are evolving and the scope of the legal rights is being broadened. To understand the concept of right to privacy we must first understand what privacy is. According to the definition, “*the right to be let alone; the right of a person to be free from any unwarranted publicity; the right to live without any unwarranted interference by the public in matters with which the public is not necessarily concerned*”⁷⁴ is called privacy of an individual. It is related to the liberty of the individual and hence related with Article 21 of the Constitution of India which states that “*No person shall be deprived of his life or personal liberty except according to procedure established by law*”⁷⁵. After drawing inference from this article, it has been interpreted that the term ‘life’ includes each of those aspects which makes a man’s life meaningful with dignity and worth living. In India the jurisprudence of the right to privacy is a latest development but over the years there have been plethora of cases which has helped it to develop.

4.7. Role of Courts: Case Analysis

Important Case Laws Which Helped To Develop Right To Privacy.

- “*M.P Sharma v. Satish Chandra*”⁷⁶

The question was raised on the constitutionality of search and seizure of document from the person against whom a FIR has been lodged, the main question was that whether this was violative of the fundamental right of that person under the “*Right to property*”⁷⁷ and “*Right against self-incrimination*”⁷⁸ of the constitution.

The bench was to ascertain that if there were any constitutional limitation to the government’s right to search and seizure and if that would somehow constitute any breach to the right to privacy of the individual.

⁷⁴ Black’s Law Dictionary

⁷⁵ INDIA CONST. Art 21.

⁷⁶ M.P Sharma v. Satish Chandra, 1954 A.I.R 3007

⁷⁷ INDIA CONST. art. 19, cl. 1

⁷⁸ INDIA CONST. art. 20, cl.3

Since the question of privacy was new and this dimension was not explored, the court while delivering the judgement did not go into the intricacies of the right, the interpretation and scope of the right was later broadened in the subsequent years. In this case the decision by an eight judge's bench held that right to privacy was not a fundamental right. The process of search and seizure in question was considered to be a reasonable restriction of freedom under the constitution which could not be held unconstitutional. It was given by the majority that the process was just a temporary interference and for that matter the statutory recognition was unnecessary.

- “*Kharak Singh v. The State of U.P.*”⁷⁹ :

Just like its precedent, only the minority opinion recognized the right to privacy as a fundamental right. Dissenting judge Justice Subbarao, said that “*even though the right to privacy was not expressly recognized as a fundamental right, it was an essential ingredient of personal liberty under Article 21. He also held all surveillance measures to be unconstitutional. The judges were of the opinion that privacy is both the right to personal liberty and freedom of movement.*”⁸⁰

The majority of the judges were of different opinion than justice Subbarao and even though after striking down the the provision allowing domiciliary visits, they held that “privacy was not a guaranteed constitutional right”. It however, held that “*Article 21 was the repository of residuary personal rights and recognized the common law right to privacy.*”

In the hindsight if we look at this case, it reeks of the “*destruction caused by the state of a sanctified personal space whether of the body or of the mind and which was violative of the guarantee against arbitrary state action*”⁸¹.

- “*R. M. Malkani vs. State of Maharashtra*”⁸²

“In 1972, the Supreme Court decided a case – one of the first of its kind – on wiretapping. In *R. M. Malkani vs. State of Maharashtra* the petitioner's voice

⁷⁹ Kharak Singh v. The State of U.P 1963 AIR 1295, 2

⁸⁰ Priyanka Mitta, *Is privacy a fundamental right? Two cases that supreme court will look at*, LIVE MINT, July 19,

⁸¹ Jayant Das, *Increasing intrusion of State into Right to Privacy*, THE PIONEER, July 04, 2018, 7:12 PM) <https://www.dailypioneer.com/2018/state-editions/increasing-intrusion-of-state-into-right-to-privacy.html>

⁸² AIR 1973 SC 157.

had been recorded in the course of a telephonic conversation where he was attempting blackmail. He asserted in his defense that his right to privacy under Article 21 had been violated. The Supreme Court declined his plea holding that “The telephonic conversation of an innocent citizen will be protected by Courts against wrongful or high handed' interference by tapping the conversation. The protection is not for the guilty citizen against the efforts of the police to vindicate the law and prevent corruption of public servants.”

- “*Govind vs. State of Madhya Pradesh*⁸³”

“*Govind vs. State of Madhya Pradesh* (1975), decided by a three-Judge Bench of the Supreme Court is regarded as being a setback to the right to privacy jurisprudence. Here, the court was evaluating the constitutional validity of Regulations 855 and 856 of the Madhya Pradesh police Regulation which provided for police surveillance of habitual offenders including domiciliary visits and picketing.” The Supreme Court desisted from striking down these invasive provisions holding that “It cannot be said that surveillance by domiciliary visit-, would always be an unreasonable restriction upon the right of privacy. It is only persons who are suspected to be habitual criminals and those who are determined to lead a criminal life that are subjected to surveillance.” The court went on to make some observations on the right to privacy under the constitution:

“Too broad a definition of privacy will raise serious questions about the propriety of judicial reliance on a right that is not explicit in the Constitution. The right to privacy will, therefore, necessarily, have to go through a process of case by case development. Hence, assuming that the right to personal liberty, the right to move freely throughout India and the freedom of speech create an independent fundamental right of privacy as an emanation from them it could not be absolute. It must be subject to restriction on the basis of compelling public interest. But the law infringing it must satisfy the compelling state interest test. It could not be that under these freedoms the Constitution-makers intended to protect or protected mere personal

⁸³ (1975) 2 SCC 148.

sensitiveness” This case is important since it marks the beginning of a trend in the higher judiciary to regard the right to privacy as “not being absolute”. From Govind onwards, ‘no absoluteness’ becomes the central defining feature of this right.

- “*Radhakrishan vs. State of U.P.*”⁸⁴

In, *Radhakrishan vs. State of U.P.* which involved an illegal search in contravention of the CrPC, the Supreme Court held that: “*So far as the alleged illegality of the search is concerned, it is sufficient to say that even assuming that the search was illegal the seizure of the articles is not vitiated. It may be that where the provisions of Code of Criminal Procedure, are contravened the search could be resisted by the person whose premises are sought to be searched. It may also be that because of the illegality of the search the Court may be inclined to examine carefully the evidence regarding the seizure. But beyond these two consequences no further consequence ensues.*”

- *Mr 'X' vs. Hospital 'Y'*⁸⁵.

“Does the disclosure by a hospital of the medical condition of an AIDS patient to his fiancé amount to a breach of the patient's privacy? This question arose in *Mr 'X' vs. Hospital 'Y'*. The Supreme Court was confronted with the task of striking a balance between two conflicting fundamental rights: the AIDS patient's right to life which included his right to privacy and confidentiality of his medical condition, and the right of the lady to whom he was engaged to lead a healthy life. The Supreme Court concluded that since the life of the fiancé would be endangered by her marriage and consequent conjugal relations with the AIDS victim, she was entitled to information regarding the medical condition of the man she was to marry. There was, therefore, no infringement of the right to privacy.”

- “*R. Rajagopal v. Union of India*”⁸⁶ :

⁸⁴ AIR 1980 SC 593.

⁸⁵ (1988) 2 All ER 648.

⁸⁶ *R. Rajagopal v. Union of India*, 1994 SCC (6) 632

“In this judgment, The right to privacy was said to be included as a part of right to life and personal liberty and the court further elaborated on whether it can be treated as fundamental right, actionable claim or both.”

“Here the court was involved a balancing of the right of privacy of citizens against the right of the press to criticize and comment on acts and conduct of public officials. The case related to the publication by a newspaper of the autobiography of Auto Shankar who had been convicted and sentenced to death for committing six murders. In the autobiography, he had commented on his contact and relations with various high-ranking police officials – disclosures which would have been extremely sensational. Sometime before the publication, he appears to have been induced to write a letter disclaiming his authorship of the autobiography. On this basis, the Inspector General of Prisons issued a letter forbidding the newspaper from publishing the autobiography claiming, inter alia, that the publication of the autobiography would violate the prisoner’s privacy. Curiously, neither Shankar himself, nor his family were made parties to this petition. The Court decided to presume, somewhat oddly, that he had “neither written his autobiography” nor had he authorized its publication. The court then proceeded on this assumption to enquire whether he had any privacy interests that would be breached by unauthorized publication of his life story. The right of privacy of citizens was dealt with by the Supreme Court in the following terms: -

“The right to privacy is implicit in the right to life and liberty guaranteed to the citizens of this country by Article 21. It is a right to be let alone. A citizen has a right to safeguard the privacy of his own, his family, marriage, procreation, motherhood, childbearing and education among other matters. None can publish anything concerning the above matters without his consent - whether truthful or otherwise and whether laudatory or critical. If he does so, he would be violating the right to privacy of the person concerned and would be liable in an action for damages. Position may, however, be different, if a person voluntarily thrusts himself into controversy or voluntarily invites or raises a controversy.”

“The rule aforesaid is subject to the exception, that any publication concerning the aforesaid aspects becomes unobjectionable if such publication is based upon public records including court records. This is for the reason that once a matter becomes a matter of public record, the right to privacy no longer subsists and it becomes a legitimate subject for comment by press and media among others. We are, however, of the opinion that in the interests of decency [Article 19(2)] an exception must be carved out to this rule, viz., a female who is the victim of a sexual assault, kidnap, abduction or a like offence should not further be subjected to the indignity of her name and the incident being publicized in press/media.”

On this reasoning, the court upheld that the newspaper’s right to publish Shankar’s autobiography, even without his consent or authorization, to the extent that this story was able to be pieced together from public records. However, if they went beyond that, the court held, “they may be invading his right to privacy and will be liable for the consequences in accordance with law.” Importantly, the court held that “the remedy of the affected public officials/public figures, if any, is after the publication”

- *“People’s Union for Civil Liberties v. Union of India”*⁸⁷ :

The SC laid down certain guidelines and regulations that such orders of the interceptions were to be only issued by the home secretaries only and only after considering the necessity of the information. This case before the Supreme Court extended the right to privacy to communications.

“People’s Union for Civil Liberties vs. Union of India, involved a challenge to Section 5(2) of the Telegraph Act, 1885 which permits the interception of messages in cases of public emergency or in the interest of public safety. The Supreme Court held that the right to privacy, which was part of the fundamental right to life guaranteed under Article 21, included the right to hold a telephone conversation in the privacy of one’s home or office.” It was held that telephone-tapping, a form of “technological eavesdropping” infringed the right to privacy. Finding that the Government had failed to lay down a proper procedure under Section 7(2) (b) of the Act to ensure procedural

⁸⁷ *People’s Union for Civil Liberties v. Union of India* (1997) 1 SCC 301.

safeguards against the misuse of the power under Section 5(2), the Court prescribed stringent measures to protect the individual's privacy to the extent possible.

The Court made the following observations:

The right privacy - by itself - has not been identified under the Constitution. As a concept it may be too broad and moralistic to define it judicially. Whether right to privacy can be claimed or has been infringed in a given case would depend on the facts of the said case.” However, the Court went on to hold that “the right to hold a telephone conversation in the privacy of one’s home or office without interference can certainly be claimed as right to privacy”. This was because “*conversations on the telephone are often of an intimate and confidential character. Telephone conversation is an important facet of a man's private life. Right to privacy would certainly include telephone-conversation in the privacy of one's home or office. Telephone-tapping would, thus, infract Article 21 of the Constitution of India unless it is permitted under the procedure established by law.*”

The court also read this right to privacy as deriving from Article 19. “*When a person is talking on telephone, he is exercising his right to freedom of speech and expression.*” the court observed, and therefore “telephone-tapping unless it comes within the grounds of restrictions under Article 19(2) would infract Article 19(1)(a) of the Constitution.”

“This case made two important contributions to communications privacy jurisprudence in India – the first was its rejection of the contention that ‘prior judicial scrutiny’ should be mandated before any wiretapping could take place. Instead, the court accepted the contention that administrative safeguards would be sufficient. Secondly, the Court prescribed a list of procedural guidelines, the observance of which would save the wiretapping power from unconstitutionality. In 2007, these safeguards were formally incorporated into the Rules framed under the Telegraph Act.”

The three judgments saw and acknowledged privacy as a constitutionally protected fundamental right, namely, *Gobind vs. State of Madhya Pradesh*⁸⁸, *PUCL vs. Union of India* (telephone tapping case) and *R. Rajagopal vs. State of Tamil Nadu*⁸⁹ (Court dealt with a conflict between the freedom of the press and the right to privacy). However, all three judgments were of smaller benches and left the stakeholders in dilemma with regards to interpretation of Privacy under Article 21 of the constitution of India or not. In Rajagopal Case the court held that the right to privacy has two aspects: the first affords an action in tort in damages for the unlawful invasion of privacy, and the second is a constitutional right.

- “*District Registrar and Collector, Hyderabad and another v. Canara Bank and another*” .

Apex court in this case did not describe the right to privacy as an absolute fundamental right but connected it with personal liberty, freedom of speech and expression and freedom of movement, and added that because of these rights which exist, the right to privacy rises.

- “*Selvi and others v. State of Karnataka and others*”⁹⁰.

This is one of the very recent examples of how the court upheld the right to privacy of an individual by giving the individual chance to go through the due process of law or the process established by law and describing the forced *narcoanalysis, brain mapping, FMRI and polygraph test* as violation of the fundamental right and unconstitutional. such forced tests were said to be self-incriminatory in nature and violative of the Art. 20(3). Interestingly, the apex court made a difference between physical privacy and mental privacy and related it to the right to privacy.

- “*Unique Identification Authority of India & Anr. v. Central Bureau of Investigation*”.

Up until this point, the development of the right to privacy as we know it today, was never perceived as the absolute one. If and when any question used

⁸⁸ (1975) 2 SCC 14.

⁸⁹ (1994) 6 SCC 632.

⁹⁰ AIR 2010 SC 1974

to arise regarding the conflict between the fundamental rights of the two parties, the right which used to advance the public morality was upheld and only that would prevail over the other.

- “*Justice K.S. Puttuswamy (Retd.) & Anr. v. Union of India & Ors.*”⁹¹.

The latest development only happened a couple of years back when along with the right to privacy; the unique identity scheme was discussed at lengths. The question raised was that whether the right of privacy was guaranteed under the constitution or not . The attorney general of Indian argued that it privacy is not a fundamental right guaranteed to Indian citizens, but, the bench was of the view that the right to privacy is a sacrosanct facet of Art. 21 of the constitution

4.8. Analysis of 2017 Judgment of Justice K.S. Puttaswamy and Anr. Vs. Union of India and Ors.⁹²

In 2017, a nine-judge bench of India’s apex court unanimously held that Privacy is a fundamental right. The court also ruled that privacy is inscribed into the Article 21 of the constitution and is intrinsic to life and liberty. The bench comprised Chief Justice Khehar and Justices A.M. Sapre, Syed Abdul Nazir, S.A. Bobde, R.K. Agrawal, R Nariman, J. Chelameshwar D.Y. Chandrachud, Sanjay Kishan Kaul and S.A. Bobde. The judges gave different arguments leading to a unanimous verdict.

In doing so, the court has overturned the *M.P. Sharma vs S Sharma* case verdict of 1958 as well as the *K Singh vs state of UP* case of 1961 where the court had denied that right to privacy is protect under the constitution.

The lead judgment of 265 pages, penned by Justice D.Y. Chandrachud and co-signed by Chief Justice Khehar and Justices Nazir and Agarwal has the below conclusions:

Conclusions of Justices J.S. Khehar, R.K. Agrawal, D.Y. Chandrachud, S. A. Nazir

⁹¹ Justice K.S. Puttuswamy (Retd.) & Anr. v. Union of India & Ors. 2017 (8) SCJ 33

⁹² AIR 2017 SC 4161.

The M.P. Sharma verdict states that the right to privacy cannot be held as a fundamental right in the Indian context under Article 20(3) since the Indian constitution does not have provisions like the 4th amendment which is enshrined in the constitution of the United States. The verdict does not clearly say if such a right may be invoked from the other provisions of the rights guaranteed by Article 19 or Article 21. It does not conclusively state that Privacy is not a fundamental right guaranteed by the constitution of India. The M P Sharma verdict is hence overruled to the extent to which it implies the contrary.

The Kharak Singh verdict has rightly stated that the expression of life as mentioned in Article 21 does not merely mean the right to an individual's "animal existence". It says that the expression 'personal liberty' is a promise against incursion into an individual's home and personal security. It rightly states that a person's dignity is an integral part of his 'personal liberty'. The

The 1st part of the Kharak Singh verdict that invalidates nocturnal domiciliary visits on grounds that it violates liberty is an implied recognition of privacy as a right. However, the 2nd part is a contradiction to the current judgement, since it says that privacy cannot be held as a fundamental right. Hence, Kharak Singh's reference of the verdict of the majority in Gopalan is not reflective of the correct position in view of the decisions in Cooper & in Menka to the extent that it holds that the privacy is not protected as a right in the constitution of India is overruled.

Life and personal liberty are the rights inextricable from a dignified human existence. Personal dignity, equality amongst people and liberty are the base of the constitution of India. However these rights are not created by the constitution, in fact, these are rights intrinsic to the human species; privacy is a right promised by the constitution of India which primarily emanates from Article 21;

Legal recognition of the constitutional right to privacy is not intended to amend the Constitution;

Privacy is intrinsic to human dignity. It has a normative as well as a descriptive function. Normative in the effect that privacy serves the values upon which the guarantees of freedom, life and liberty are founded. Descriptive in the effect that privacy suggests a list of entitlements which forms the foundation of liberty;

Essentially, privacy preserves personal intimacy, sanctity of life, marriage, procreation and sexual orientation. It is also a right to be left alone. It protects personal autonomy and relies on the right and ability of the person to control his life. Our plural and heterogeneous culture is protected by privacy.

It is critical to emphasize that privacy is not yielded merely by an individual's presence in a public area. This is true even though the hopes of it may change from intimate/private spaces to public areas. The right to privacy still holds because of its inseparability from human dignity.

The intention is not to promise a list of entitlements in the right to privacy but that to evolve when needed to protect privacy of an individual. The perceptions during the adoption of the constitution cannot be held as timeless wisdom, with new challenges birthed by technological advances, many ideas of the past and present may become obsolete. Hence the basic features of constitution must always be upheld with the help of flexible interpretations for the progeny;

As is the case with other fundamental rights like the right to life and personal liberty under Art. 21, the right to privacy also is not absolute. Permissible curtailments of fundamental rights need to be taken into account in the event of a new law. Meaning, any intrusion into personal privacy must be justified as fair before any law can be enacted. Similarly, it should not encroach upon the right to life and personal liberty under Article 21;

Right to privacy has two aspects: On one hand it means that the state must not intrude upon the life and personal liberty of an individual. On the other hand it defines the protection of individual privacy as a duty of the state.

The verdict subsequent to Kharak Singh case, upholding the right to privacy would be subject to the principles stated above.

The challenges to privacy are not only limited to the state but also from non-state agencies. Hence regime to protect personal data becomes necessary on the part of the Government of India. Such regime would need to find equilibrium between personal rights to privacy and legitimate concerns of the state. The latter may include national security, crime, business interest, etc. It has been brought to court's notice that the government has already made a committee headed by Honourable Justice B.N. Srikrishna, a former judge of the Supreme Court.

Petitioners' Arguments

Contention that the collection of biometric data for Aadhaar cards risks exposure, issue and is in violation of the fundamental right to privacy put forth by the petitioners, former Karnataka high court judge Justice K.S. Puttaswamy and others.

Prominent advocates G Subramaniam, S Divan, S Pooyaya, A Grover & Indira Jaising and former attorney general S Sorabjee made the followed arguments on the petitioners' behalf:

1. Right to privacy would be included in the right to life under Article 21 of Indian constitution though it has not been clearly specified.
2. Protection of personal information is an aspect of privacy but it cannot be regarded as the complete definition of privacy. Subramaniam argued, "Privacy is about the freedom of thought, conscience and individual autonomy and none of the fundamental rights can be exercised without assuming certain sense of privacy".⁹³ Protecting the fundamental rights of the people is an affirmative obligation of the state. "Liberty is fundamental to democracy and citizens cannot exist without privacy."
3. Sorabjee stated, "Privacy is not explicitly laid out in the constitution. But that does not mean the right does not exist as it has been deduced from the constitution". He held the derivation of the freedom of press from Art. 19

⁹³ Right to Privacy
<http://thelegiteye.in/2017/10/24/case-analysis-right-privacy>. (visited on Feb 22, 2018)

as a precedent to argue that right to privacy may also be derived similarly from Art. 21

4. The advances of technology has made it necessary for an individual to have control on the extend to which he/she wishes to share personal data. A lacm of protection of personal data results in an intrusion to privacy.
5. Arun Jaitley, the finance minister in the Union government has cleary stated during the discussions held for Aadhar Bill in the Rajyasabha in 2016 that right to privacy is a fundamental right. A stand which is contradictory to the current position of the government.
6. Subramanium argued, “Liberty existed prior to constitutional era and the law had merely recognized its existence. Liberty, which is fundamental to democracy and citizens, cannot exist without privacy”.

Attorney General’s Arguments

The attorney general KK Venugopal, speaking on Centre’s behalf, pointed out that a bench of eight judges in 1954 and a bench of six in 1962 had clearly stated that right to privacy was not a fundamental right.

He stated that right to privacy cannot be claimed as a funadamental right under Art. 21, Art, 14 or Art. 19, although it was a fundamental right under the British Common Law.

The nationality and vagueness of the concept of privacy was brought to the attention of the court as a hindrance with it being qualified as a fundamental right. “Every aspect of it does not qualify as a fundamental right, as privacy also includes the subtext of liberty. No need to recognize privacy as an independent right. Defining the contours of privacy is not possible. Privacy is as good a notion as pursuit of happiness,”⁹⁴

“If privacy were to be declared a fundamental right, then it can be a qualified right.” It was argued that privacy is a limited fundamental right that can be restricted subject to state interest. It was argued that in Indian context, other fundamental rights like food, clothing, etc are far more important.

⁹⁴ *Ibid.*

“The government said Aadhaar would not fall under the right to privacy. We can’t say every encroachment of privacy is to be elevated to fundamental right. The claim to liberty has to subordinate itself to right to life of others,” he said.

He referred to a statement by the World Bank that an identity system is needed in developing countries as a counter to arguments against the Aadhar Card system.

This reference is answered by stating that the inalienable fundamental right to privacy resides in Article 21 and other fundamental freedoms contained in Part III of the Constitution of India. M.P. Sharma⁹⁵ and the majority in Kharak Singh⁹⁶, to the extent that they indicate to the contrary, stand overruled.

As a result a return to later judgements regarding privacy as a right is not necessary. Hence these cases are returned for adjudication on grounds to the bench of three hon’ble judges of the court in light of the current judgement.

⁹⁵ Supra note 35.

⁹⁶ *Ibid.*

CHAPTER 5

NATIONAL SECURITY LEGISLATIONS AND THEIR EFFECT ON PRIVACY

5.1. The Unlawful Activities (Prevention) Act, 1967

5.1.1. A Brief History of the UAPA

Dissent and Opposition are one of the core values of every existing democracy in the world. They are one of the very basic principles on which democracy is based. But, there is a very thin line of difference between Dissent and Violence, and when one crosses the said line, terrible things are bound to happen, take Pakistan and Bangladesh for example. The need for the Unlawful Activities Prevention Act arose when the National Integration Council appointed the committee on National Integration and Regionalism. The sole purpose for constituting the committee was to look into the issues concerning the Sovereignty and Integrity of India. This further led to the passing of the 16th Amendment to the Constitution of India, which then put reasonable restrictions upon the Fundamental Rights which were guaranteed by Article 19 of the Constitution of India. The said act was passed in the wake of the defeat which India suffered at the hands of the India-China war of 1962, and for the purposes of maintaining the sovereignty and integrity of India, because at that time, the DMK Party was contesting elections from the Tamil Nadu state, and it posed a great threat to the sovereignty of India because secession from India was a part of their election manifesto.

The Unlawful Activities (Prevention) Act, 1967 was the Government of India's first legislation which was targeted at countering terrorism and anti-national activities within the territory of India. With the passage of time, the act was amended several times.

Although legislated for the benefit of the nation, the UAPA started gaining active criticism from 2004 when the said amendment was passed, which contained a majority of the provisions from the repealed Prevention of Terrorism Act (POTA). This criticism only went upwards from that point,

calling the act out as fascist, and outright unconstitutional. The reasons for the same aren't wrong as well, because the government has time and again made arbitrary arrests within the scope of the said act. Furthermore, the act has been criticized of using very vague and open ended terms to define simple things, just so that arrests can be made under this act for a wide range of acts without they actually being something considerate or not.

5.1.2. Reasons for Legislating the Unlawful Activities (Prevention) Act, 1967

As very well stated earlier, there were many reasons which were considered before the passing of the UAPA. These reasons were:-

- **Defeat in the Sino-Indian War:** The Indian Army was heavily unequipped during the Sino-Indian war, and the Chinese were far advanced in their military technologies as well as their equipment.⁹⁷ This led to heavy losses on the Indian Side. The aftermath of the battle resulted in India losing a significant portion of the Kashmir Valley, known as Aksai Chin, to the Chinese. This was a big blow to the sovereignty of India, and a grave concern to the government back then.
- **Rising Insurgency in India:** Communists and Chinese Sympathizers were already starting to assimilate in 1955-56 within West Bengal. India was already in the process of inculcating the Princely States with the territory of India, and there was already a growing sense of discontentment within the Princely States which were already a part of India, because the Government wasn't living up to the promises which were made to them while ceding their territory to India. There were even more radical insurgencies rising in the State of Nagaland, claiming direct secession from India.⁹⁸
- **DMK Contesting Elections in Tamil Nadu:** The DMK Party at that time planned on contesting the elections for the State Legislature of Tamil Nadu.

⁹⁷ Maj Gen Sheru Thapliyal, *1962 War: A Critical Analysis*, Mar. 30, 2018,

<http://www.indiandefencereview.com/spotlights/1962-war-a-critical-analysis/> (Last Visited: 01st August, 2020)

⁹⁸ Namrata Goswami, *Indian National Security and Counter-Insurgency: The Use of Force Vs Non-violent Response*, ROUTLEDGE, 43. ISBN 978-1-134-51431-1

Tamil Nadu was already a part of India at time, and there was a growing sense of discontentment amongst the people of Tamil Nadu because the Government of India had not agreed to separate the states on the basis of language as promised. This became the topmost agenda of the DMK Party, and officially in their Election Manifesto DMK declared that if they win the elections, they will be moving for a secession from the Indian Territory.⁹⁹

These reasons started worrying the Indian Government, because that was a time when India wasn't even geopolitically as we see. The territories of Goa, Pondicherry, and even Sikkim weren't a part of India, while the states like Mysuru and Cochin kept demanding further division on the basis of language. This combined with a loss of territory in Aksai Chin had the Government worried about any further losses to the Sovereignty and Integrity of India. Hence the Government, after amending the Constitution through the 16th Amendment Act, and putting reasonable restrictions on the rights provided under Article 19 of the Constitution of India, moved forward with introducing the Unlawful Activities (Prevention) Act, 1967.

5.1.3. Why was the UAPA unique?

Several provisions of the Unlawful Activities (Prevention) Act, 1967, were authoritative, as well as overly broad in their definition, thereby allowing the government to do a large number of things over a simple authority, just because it wasn't specific enough to point out as to what it was actually referring to.¹⁰⁰

Further, certain things which made the UAPA stand out from other legislations at that time are:-

- **Declare All-India bans on organizations and associations:** By far the most distinct and the most used feature of the UAPA is the power which the act gives to the government to impose an All-India Ban on Organizations. The

⁹⁹ ROBERT L. HARDGRAVE, JR., THE DMK AND THE POLITICS OF TAMIL NATIONALISM, Pacific Affairs, Vol. 37, No. 4 (Winter, 1964-1965), 396-411

¹⁰⁰ Unlawful Activities (Prevention) Act, 1967, Sec 2, Sec 3

Government, by virtue of Section 3 of the act could simply announce that an association is unlawful, by publishing a notice in the Official Gazette, if it is of the opinion. The section further goes on to provide that the government has to provide the reasons as to which it opined that the association is unlawful. However, the proviso to the same subsection provides that nothing in the said clause could mandate the Government to give reasons for banning an association if the Government is of the opinion that declaring such reasons to the public shall not be in the public interest to disclose.¹⁰¹ This essentially gave the Government the power to declare any organization as unlawful and not give any justification whatsoever as to why it chose to declare it as such.

- **Vague and Open Ended Interpretation to clauses:** Section 2(f)¹⁰² of the Unlawful Activities (Prevention) Act, defines the term Unlawful Activity, as any act which intends to bring about cession or secession to any part or territory of India, or which incites an individual or association to do so, or it does anything to harm the sovereignty and integrity of India. Now this definition in itself opens up hundreds of interpretations, because nowhere in the said legislation has any act been defined which could be seen as an act harming the sovereignty or integrity of India. Further, Section 2(g)¹⁰³ defines an unlawful organization as any organization which does unlawful activity, or whose members do such activity, or which aids in committing of such activity.
- **Harsh and Unreasonable Punishments:** Section 10 of the Unlawful Activities (Prevention) Act, provides that any person who is merely a member of an unlawful association can be punished with imprisonment up to 2 years. Section 13, on the other hand, punishes who takes part, abets, advises, or incites the commission of any unlawful activity with an imprisonment of up to 5 years.
- **Arrests without Warrants:** Section 14 of the Unlawful Activities (Prevention) Act, 1967, clearly states that any offence which is listed under this act shall be cognizable only. This therefore allows the police to arrest a

¹⁰¹ “Provided that nothing in this sub-section shall require the Central Government to disclose any fact which it considers to be against the public interest to disclose.”

¹⁰² Section 2(o) in the present act.

¹⁰³ Section 2(p) in the present act.

person whom they suspect of being linked to an unlawful association, without a warrant. Not only an arrest, but the police can actually go further and started an investigation without even the permission of the court. This actually in turn grossly overpowers the police in matters related to Unlawful Activities, and the police can misuse the powers for harassing people and activists without any valid reasons or authority to do the same.¹⁰⁴

- **Protection from Civil Liability:** To put the final nail to the coffin, the Government actually went forward and included Section 18¹⁰⁵ of the Unlawful Activities (Prevention) Act, 1967, which stated that No Legal Proceeding shall lie against the government for any loss or damage caused because of any action taken by the Government while acting under the powers of the said act. This actually gave the government full immunity from any kind of responsibility which may arise from the continuous use of the said act.

The act did provide some relief, with provisions for establishment of a Tribunal in the case of unjustly ruling an organization a terrorist organization, but little to no relief has been provided through such tribunals, and an organization which had made its way to be banned under this act has in the end remained banned. The SIMI is a living example of such act.¹⁰⁶

5.2. Similar Legislations as the UAPA

Although the Unlawful Activities (Prevention) Act as of today deals not only with Unlawful, but terrorist activities as well, the same wasn't always the case when it came to dealing with terrorism and related activities. Prior to inclusion in the UAPA, terrorist activities within the Territory of India were dealt with the Terrorism and Disruptive Activities (Prevention) Act, 1987. This act was brought in by the Parliament after increasing insurgency in the Punjab region

¹⁰⁴ Vishwa Mohan & Anam Ajmal, “Cops use UAPA to block site, call it ‘goof-up’ later”, The Times of India, Jul 24, 2020
http://timesofindia.indiatimes.com/articleshow/77137573.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

¹⁰⁵ Section 49 of the Present UAPA Act.

¹⁰⁶ Union of India v. Students Islamic Movement of India, 2002 SCC OnLine Del 340

due to Bhindrawale.¹⁰⁷ TADA was the first act in India which actually went on and defined terrorism and what it was. TADA defined terrorism as:-

“Whoever with intent to overawe the Government as by law established or to strike terror in the people or any section of the people or to alienate any section of the people or to adversely affect the harmony amongst different sections of the people does any act or thing by using bombs, dynamite or other explosive substances or inflammable substances or lethal weapons or poisons or noxious gases or other chemicals or by any other substances (whether biological or otherwise) of a hazardous nature in such a manner as to cause, or as is likely to cause, death of, or injuries to, any person or persons or loss of, or damage to, or destruction of, property or disruption of any supplies or services essential to the life of the community, or detains any person and threatens to kill or injure such person in order to compel the Government or any other person to do or abstain from doing any act, commits a terrorist act.”¹⁰⁸

Post the coming in force of TADA, this act was heavily misused, and its unpopularity started rapidly increasing, because it led to a number of arbitrary arrests, and misuse by the police force. Apart from this, the TADA had a number of other faulty features which were grossly unconstitutional and outright immoral. For example, the act provided that a person can be detained for up to 1 year without any formal charges being pressed on him. The Act further provides that a detainee can be in the custody of the police for upto 60 days, and post than even, he needs not to be presented before a magistrate, but an Executive Magistrate.¹⁰⁹ Furthermore, the act reverses the presumption of innocence, stating that a person caught under this act is presumed guilty until his innocence is proven otherwise.¹¹⁰ Lastly, any person who is tried under this

¹⁰⁷21 K.P.S. GILL, ENDGAME IN PUBJAB: 1988-1993, (Ajai Sahni)

<https://www.satp.org/satporgtp/publication/faultlines/volume1/Fault1-kpstext.htm>

¹⁰⁸ Terrorist and Disruptive Activities (Prevention) Act, 1987, Sec 3(1).

¹⁰⁹ Terrorist and Disruptive Activities (Prevention) Act, 1987, Sec. 20.

¹¹⁰ Terrorist and Disruptive Activities (Prevention) Act, 1987 ,Sec. 21.

act cannot appeal anywhere, except to the Supreme Court of India.¹¹¹ For reasons such as this which are so immoral, the act was allowed to lapse in 1995 when it was due for renewal. During the 7 years TADA remained in force, 76000 people were arrested in India under the act.¹¹² Of the people arrested, 25 percent of the cases were dropped by the police without even any formal charges being pressed, while only 35 percent of the cases were brought to trial, resulting in 95 percent conviction. In essence, less than 2 percent of the people who were arrested were actually convicted.¹¹³ This shows how the police abused their power when armed with the TADA. This act lapsed in 1995, and was further repealed by the Prevention of Terrorism Act, 2002.

In *Kartar Singh v. State of Punjab*¹¹⁴, the validity of TADA was challenged on the ground that it dealt with the issue of 'public order', which was within the legislative domain of states. Nevertheless, the Court upheld the validity of TADA. The Court held that 'public order' covered issues of lesser gravity and more serious threats covered in TADA fell within the Union's domain relating to national defence.

A similar challenge was mounted against POTA in *PUCL v Union of India*¹¹⁵, which too was repelled by the Court on similar grounds.

The Prevention of Terrorism Act, 2002, was passed by the parliament after a lot of controversy because of the already misused Prevention of Terrorism Ordinance, 2001. The Ordinance was passed in the wake of the 2000 Red Fort attack and the 2001 Parliament Bombings. The Ordinance already came under a lot of criticism when the police started overreaching their powers and misusing the provisions of the act. The Bill to make this Ordinance into an act

¹¹¹ Terrorist and Disruptive Activities (Prevention) Act, 1987, Sec 19.

¹¹² ZAIDI, S. HUSSAIN, *BLACK FRIDAY – THE TRUE STORY OF THE BOMBAY BOMB BLASTS*. (Penguin Books. ISBN 978-0-14-302821-5)

¹¹³ *Id.*

¹¹⁴ AIR 1961 SC 1787

¹¹⁵ 1997 (1) SCC 301

failed at the Rajya Sabha,¹¹⁶ but was later passed by a joint session of the Parliament.

Just like the TADA, POTA also had the provision for holding a person in custody for up to 180 days without any filing of the chargesheet. Further, the laws in India do not accept any confession made to a police officer as evidence, and allow it to be rebutted in trial. This was however not the case in POTA, and every confession made to a police officer is admissible and can be used against a person in trial. POTA was misused heavily by the government, and the police itself misused the act to torture and humiliate prisoners.¹¹⁷ POTA was later repealed in 2004 when the Government at the center changed.

5.3. Further Amendments to the UAPA, making it as Draconian as it stands

The first substantial amendment to the UAPA was introduced in the year 2004, when the Congress Government, as promised, repealed the POTA. However, the repealing of the POTA had little to no difference in the status quo, because almost a majority of the provisions of POTA including those relating to ‘Terrorism’, ‘Terrorist Organization’, ‘Terrorist Act’ etc. were all inculcated in the UAPA. The Schedule of POTA which listed all the Terrorist Organizations was also added to the UAPA. POTA’s definition of terror afflicts UAPA too. It is defined primarily through intent (“intent to strike terror”), others things being same. It duplicates a range of criminal law offences, such as causing death, injuries, damage to public property, disrupting essential services, use of firearms, explosives etc—all of which are otherwise also covered under a range of laws.¹¹⁸ This provides latitude to the executive—both police and government—to subjectively choose what to designate as terror, and what to dismiss indulgently as ordinary violence. It is in their power then to decide

¹¹⁶Editorial, “*It’s not POTA, yet,*” Outlook, Mar 21, 2002

<https://www.outlookindia.com/website/story/its-not-pota-yet/214958> (Last Visited 01st August, 2020)

¹¹⁷ Nitya Ramakrishnan, *Excerpt | Tortured, Humiliated, But Unbroken: An Interview With S.A.R. Geelani*, <https://thewire.in/rights/sar-geelani-custodial-torture-nitya-ramakrishnan> (Last Visited: 01st August, 2020)

¹¹⁸ Unlawful Activities (Prevention) Act, 1967, as amended in 2019, Sec. 15-23

when to invoke the draconian provisions of UAPA, and when to apply (and in some cases, never to apply) ordinary criminal law.

What the UAPA hollows out is the constitutional guarantees of fair trial and right to life and liberty. It thus perverts the very notion of rule of law beyond recognition. Section 43D(5) of the UAPA, which deals with bail provisions. A replica of Section 49(7) of POTA, it makes it practically impossible for an accused to secure bail. Under this section, bail cannot be granted till the public prosecutor has been heard, and it can be declined if the magistrate concludes, upon reading the charge sheet, that the charges are true. So, in effect, an accused has to demonstrate her innocence, that too at the start of the trial, in order to be even granted bail. UAPA thus explicitly—and legally—denies the presumption of innocence. Which, of course, is the very bedrock of modern law.

After 2008 terrorist attack in Mumbai, some provisions of the repealed POTA and TADA were once again added to the UAPA. These provisions were the ones referring to the time a person can be detained in police custody.¹¹⁹ The 2012 amendment to the UAPA further went on to expand the definition of terrorism to include offences which harmed the economic security of the nation too.

5.3.1. The Final Immoral Amendment in 2019

“The most recent amendment that came was the Unlawful Activities (Prevention) Amendment Act, 2019 which dealt with expanding the definition of terrorist to include individuals under Section 35 and 36 of Chapter VI of the Act. It allows the DG of NIA seizure of property from proceeds of terrorism under Section 25 and the powers of officers with the rank of inspectors and above to investigate cases under UAPA Section 43. A Review Committee to denotify the individual notified as a terrorist is also constituted by the Central Government thus removing all the chances of any institutional mechanism for judicial review.”

¹¹⁹ Unlawful Activities (Prevention) Act, 1967, as amended in 2019, Sec. 43D(2)(b)

“The primary objections to the Amendment are under Section 35, in addition to the categorization of organizations as terrorist organizations, extended the power to include within its scope the categorization of individuals as terrorists as well. Secondly, the new Amendment is contrary to the principle of ‘innocent until proven guilty’ and also violates the International Covenant on Civil and Political Rights, 1967¹²⁰ which recognizes the mentioned principle as a universal human right. Thirdly, it is being used to repress rather than combat terrorism since the amendment provides that designation of an individual as a terrorist would not lead to any conviction or penalties.” Fourthly, no objective criterion has been laid for categorization, and the government has been provided with “unfettered powers” to declare an individual as a terrorist.

5.3. Abuse of powers granted by UAPA and Legal Challenges

The most prominently abuse of the Unlawful Activities (Prevention) Act can be seen when the Delhi Police arrested Umar Khalid, a student leader at the Jawaharlal Nehru University in connection with hatching a conspiracy to create communal violence over the Citizenship Amendment Act. The Delhi Police further went on to arrest Meeran Haider and Safoora Zargar under the same draconian provisions. The police said that they were all key in premeditating a conspiracy to start riots in the national capital.

The Jammu and Kashmir Police arrested the Journalist Masrat Zahra under Section 13 of the Unlawful Activities (Prevention) Act, 2020 by stating that she uploaded anti-national videos on Facebook to incite the youth in glorifying anti-national activities. They also put this same draconian provision on Peerzada Ashiq when she posted about the diversion of COVID testing kits, stating that it is against the authorities. The Amnesty International Executive Director called such acts by the Indian Government as an attempt to curb the right to freedom of expression of its citizens.¹²¹

¹²⁰ International Covenant on Civil and Political Rights, 1976. Art. 14, cl. 2.

<https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx> (Last Visited: 01st August, 2020)

¹²¹“*J&K Police Using Repressive Counter Terrorism Law To Muzzle Access To Social Media*”, Amnesty International India, Feb 18, 2020.

“The Jammu and Kashmir police had also invoked Section 13 of UAPA against people who were accessing social media through VPN’s to dodge the longest ever internet ban imposed by the government when it scrapped Article 370 of the constitution to divide the state into two centrally administered UT’s.”¹²² The government said that it was done “to curb the misuse of the sites by miscreants for propagating false information/rumors.”¹²³

The Supreme Court has scrutinized specific provisions of the above legislations on various occasions. For instance, the Court in *“Sri Indra Das v. State of Assam”*¹²⁴, read down Section 10 of UAPA and Section 3(5) of TADA, both of which made mere membership of a banned organization, criminal. The Court held that, *“A literal interpretation of these provisions would make them violative of Articles 19 and 21 of the Constitution. This was in line with the previous decision in Arup Bhuyan’s”*¹²⁵ case where the Court had held that ‘mere membership of a banned organisation will not make a person a criminal unless he resorts to violence or incites people to violence or creates public disorder by violence or incitement to violence’.

“Manifest arbitrariness, therefore, must be something done by the legislature capriciously, irrationally and/or without adequate determining principle. Also, when something is done which is excessive and disproportionate, such legislation would be manifestly arbitrary. We are, therefore, of the view that arbitrariness in the sense of manifest arbitrariness as pointed out by us above would apply to negate legislation as well Under Article 14.”¹²⁶

<https://amnesty.org.in/news-update/jk-police-using-repressive-counter-terrorism-law-to-muzzle-access-to-social-media/> (Last Visited: 01st August, 2020)

¹²² Deepali Bhandari & Deeksha Pokhriyal, *The Continuing Threat of India’s Unlawful Activities Prevention Act to Free Speech*, JURIST, Jun 2, 2020.

<https://www.jurist.org/commentary/2020/06/bhandari-pokhriyal-uapa-free-speech/>

¹²³ Editorial, *“Panic in Kashmir as case filed against social media users”*, Al-Jazeera, Feb 18, 2020.

<https://www.aljazeera.com/news/2020/02/panic-kashmir-cases-filed-social-media-users-200218114417864.html>

¹²⁴ (2011) 3 SCC 380.

¹²⁵ Arup Bhuyan v. State of Assam, (2015) 12 SCC 702.

¹²⁶ Shayara Bano v. Union of India, (2017) 9 SCC 1.

A Public Interest Litigation has been filed by one Sajal Awasthi¹²⁷ asking the Supreme Court to declare the UAPA as unconstitutional because it is violative of the Fundamental Rights of the citizens. He goes on to explain that the right to dissent is one the very basic rights of an individual and the curtailing the same would be grossly against Articles 14,19, and 21 of the Constitution of India. He also states that the act does not provide any opportunity to the person arrested to prove that he is not a terrorist, which is very arbitrary to the core. He further went on to say that:-

“Right to Reputation is an intrinsic part of [a] fundamental right to life with dignity under Article 21 of the Constitution of India and terming/tagging an individual as ‘terrorist’ even before the commencement of trial or any application of judicial mind over it, does not adhere to procedure established by law.”

The Association for Protection of Civil Rights (APCR) filed another petition in the Supreme Court challenging Section 35 of the UAPA, because after the 2019 amendment it allows the Government to label an individual as a terrorist, whilst before the same could only be done to organizations and associations.

5.4. Privacy Concerns over the Said Acts

Questionable Legislations such as the UAPA, TADA, POTA etc. have always been surrounded with a question of overreach. The said overreach in this scenario is that to what extent these said acts would go in order to breach the privacy of the individual. The UAPA till today itself post the 2019 amendment has been criticized on numerous occasions for having little to no regard for the privacy of a person whom they just ‘suspect’ of some act. In simpler words, the UAPA empowers the investigating agencies to do any act and breach the privacy of an individual if they deem so reasonable after suspecting the said individual.

¹²⁷ Sajal Awasthi v. Union of India https://www.livelaw.in/pdf_upload/pdf_upload-363231.pdf

An instance of the UAPA being misused of such a horrendous act would be when the Delhi Police barged directly into the home of the AISA President Kanwalpreet Kaur and seized her mobile phone stating that it was required as a part of the investigation under the Delhi Riots. When she was handed the seizure memo, along with a bunch of charges, a few charges were also placed under the UAPA for seizing her mobile phone.¹²⁸

The UAPA has also been criticized by the United Nations Special Rapporteurs for violating the privacy of a said individual. The amended Act allows for searches, seizures and arrests based on the “personal knowledge” of police officers without a written validation from a superior judicial authority. The police are empowered by the amendments to enter the premises on a person on the mere suspicion of her being part of an “unlawful association”. The police have the power to examine the books, and other properties of the accused and also make enquiries against her. This, the statement declares, is a clear violation to the right to privacy as per India’s international law obligations.¹²⁹

The Act also interferes with the privacy and liberty of individuals contravening the provisions which protect against arbitrary or unlawful interference with a person’s privacy and home. The Act allows for searches, seizures and arrests based on the ‘personal knowledge’ of the police officers without a written validation from a superior judicial authority.¹³⁰ This interferes with the privacy and liberty of individuals which is not only by a fundamental right but also contravenes the provisions of the International Convention on Civil and Political Rights (ICCPR)”, which protects against arbitrary or unlawful interference with a person’s privacy and home.

If such acts aren’t horrendous enough, the UAPA has also been used on little things such as the use of a VPN. The Jammu and Kashmir Police actually arrested people under the UAPA from Jammu and Kashmir for allegedly using

¹²⁸ Editorial, “*Police bid to intimidate Kawalpreet, claims AISA*”, The Hindu, Apr 29, 2020

¹²⁹ Ujjaini Chatterji, “*UN Special Rapporteurs express concerns over UAPA*,” THE LEAFLET, May 18, 2020. <https://theleaflet.in/un-special-rapporteurs-express-concerns-over-uapa/>

¹³⁰ Aakar Patel, “*UAPA (Amendment) Bill 2019 violates the very international laws it quotes, defies principles of natural justice*,” FIRSTPOST, Aug 03, 2019. <https://www.firstpost.com/india/uapa-amendment-bill-2019-violates-the-very-international-laws-it-quotes-defies-principles-of-natural-justice-7104391.html>

the internet through a VPN. If that is not enough too, the people who were arrested were actually slapped with not only the UAPA, but also the repealed provision Section 66A of the IT Act. For a common man with little to no legal knowledge, committing such acts is a horrendous abuse of power, and harassment of individuals while imposing a totally authoritarian regime for them to live in.¹³¹

Such concerns have not solely been with the UAPA itself, other acts previously existing in the Republic of India also had such serious flaws in them which literally allowed them to step over the right to privacy of an individual. Under Section 7 of the POTA, a police officer investigating an offence under POTA can seize or attach any property if he has reason to believe that such property constitutes the proceeds of terrorism. The fear that's permitting a police officer to act on the basis of his belief is "draconian and unguided".

Section 14 requires any officer or authority of the Central or a State government, other organisations and institutions, and even individuals to furnish to an investigating officer information relating to such an offence, and makes the failure to do so an offence. This provision is against Article 20 of the Constitution, besides being an onslaught on individual freedom and right to privacy.

Chapter V of POTA deals with the interception of electronic communications, which also creates an audit mechanism that includes some provision for judicial review and parliamentary oversight; however, it remains to be seen how effective such mechanisms will be in practice. In certain high-risk states such as Jammu and Kashmir, search warrants are not required and the government from time to time bans the use of cellular telephones, long distance phones, and cyber-cafes.¹³²

¹³¹“*J&K Police Files FIR under UAPA against Those Accessing Social Media*”, the Wire, Feb 18, 2020.

¹³² The Prevention Of Terrorism Act, 2002, No. 15 of 2002.

<http://www.satp.org/satporgtp/countries/india/document/actandordinances/POTA.htm>.

Just because POTA gave police broad, if not indiscriminate, powers of arrest and detention for a variety of ill-defined and constitutionally untested offenses, Indian citizens had far more to fear than infringements upon their privacy. The extent of POTA's abuse proved that fear of prolonged, arbitrary detention was not unfounded or conjectural.

The Right to privacy of an individual has to be protected, and so has been time and again said by the courts. There have been numerous judgments wherein the courts have asked the government to make laws in accordance with protecting the privacy of an individual, but the government has somehow or the other managed to get away without actually doing something to protect the rights of an individual. The Supreme Court has stressed upon the fact that "it is entirely for the Central Government to make rules on the subject of interception but till the time it is done the right to privacy of an individual has to be safeguarded."¹³³

The Maharashtra Control of Organized Crime Act, 1999 has provisions for interception and safeguards for the same. These provisions and their safeguards similar to the directives laid down by the Supreme Court in PUCL's case. The court observed that though the interception of communications is an invasion of an individual's right to privacy, the right to privacy is not absolute, thus the court is required to see that the procedure itself is fair, just, and reasonable. Pursuant to the procedural safeguards formulated by the Supreme Court in the P.U.C.L case, the Central Government brought out an amendment to the Indian Telegraph Rules, 1951 but failed to remove unguided interception. To fill the procedural gap the interception powers laid out in the Information Technology Act were amended in 2008, and in 2009 the IT Procedure and Safeguards for Interception, Monitoring, and Decryption of Information Rules, 2009 ("IT Interception Rules") were notified. The above two development has supplement the procedural lacuna of Unlawful Activities (Prevention) Act, 1967, 2004, 2008 and 2012 as far as the procedure for interception is concern. Even the National Investigation Agency may use the power of interception but only with the procedural safeguard

¹³³ People's Union of Civil Liberties Vs. Union of India, AIR 1997 SC 568

which now included under the IT amendment 2008 and IT Interception Rules 2009.¹³⁴

5.5. Peroration

There has always been a need for a strong hand to counter terrorism and all such related activities, but if the protection for the citizen came at a cost of gross miscarriage of justice and violating the basic human, if not fundamental rights of an individual, then what good does such a protection do? The Right to Dissent is one of the core founding principles on which democracies are built, and the UAPA simply tries to take away that right from the people. It is an assault of citizens' right to expression which is also a collective right of groups and unions to disseminate their views and UAPA majorly targets this right. Secondly, it can simply be used to bypass fundamental rights and procedures. For instance, those arrested under UAPA can be incarcerated up to 180 days without a charge sheet being filed. It thus directly violates Article 21 of the constitution. Thirdly, it confers upon the government broad discretionary powers and also authorizes the creation of "special courts with the ability to use secret witnesses and to hold closed-door hearings."¹³⁵

Like the TADA and POTA, UAPA also criminalises ideology and association. By virtue of declaring an organisation 'unlawful' or 'terrorist' and banning it, these Acts have *de facto* criminalised their ideologies. Hence mere possession of any literature of such an organisation or even upholding an ideology common to that organisation in the absence of any violent act is construed as an offence. On the other hand, mere membership or association with such an organisation too becomes an offence. It is by this logic, that very often, organisations advocating the rights of a certain minority community or that of oppressed sections are easily labelled as fronts of a proscribed organisation under the schedule of the Act. Their activists or members get arrested and remain in prison for years, and are denied bail.

¹³⁴ State of Maharashtra Vs. Bharat Shanti Lal Shah and others, (2008) 13 SCC 5

¹³⁵ Chapter VII of the Unlawful Activities (Prevention) Act, 1967. As amended by the 2010 amendment.

Desperate times indeed call for desperate measures, and history is a brave example that no matter how desperate one gets, nothing is above the human rights of an individual. The way the UAPA has been drafted clearly puts it in par with the USA PATRIOT Act, which was criticized way too much for being violative of fundamental rights.¹³⁶ In essence, from a neutral standpoint, there is no way an act like the UAPA should exist in a democracy like India, unless we are already an Orwellian State like the US.

5.6. UAPA as a law being misused

The UAPA as a law has been used on several instances to harass, arbitrarily arrest, or even influence people to do certain acts against their will. While we live in a country where the rule of law is valued and upheld the most, certain acts which have been committed by the government and the investigating agencies make us lower our heads in shame.

In the year 2006, a man called Abdul Wahid Sheikh was arrested by the Mumbai ATS for his alleged involvement in the 2006 Mumbai Train Blasts. What transpired after the said arrest is a horror story for the most of us. He was constantly tortured, abused, harassed, and denied medical care while the investigation was going on and no formal charges were pressed. Internationally banned techniques such as waterboarding were used in order to force confessions out of him. In the year 2015, he was finally acquitted after spending 9 years in jail on false charges. This shows the heights to which the UAPA can be manipulated.¹³⁷

In the year 2011, the ATS arrested members of the artistic group Kabir Kala Manch (KKM) for their alleged involvement with the Maoists. Several of their

¹³⁶ Dustin Volz, “*Opposing Trump, conservative bloc demands reforms to internet spy law*” , REUTERS, Jun. 16, 2017.

<https://www.reuters.com/article/us-usa-intelligence/opposing-trump-conservative-bloc-demands-reforms-to-internet-spy-law-idUSKBN1962SR> (Last Visited: 01st August, 2020)

¹³⁷ Abdul Wahid Shaikh, *Interview: Of Torture, Impunity and the False Charges on Abdul Wahid Shaikh* ,THE WIRE, May 20, 2017.
<https://thewire.in/law/abdul-wahid-shaikh-acquitted-interview>

members have since been arrested, solely for the reason of writing songs on social issues. The Bombay High Court has refused to grant bail to any of the accused, solely because a person charged under the UAPA has to prove his innocence, and the onus of proof is upon him rather than the state.¹³⁸

On 9th May 2014, a Professor of the University of Delhi, Dr. G.N. Saibaba was arrested under the UAPA. What's shocking is the fact that the arrest wasn't made through proper legal channels, rather, he was abducted while he was on his way home. His family wasn't informed of the arrest either. He has since been kept in solitary confinement, and for a man who is 90% disabled, this is way too excessive. The only reason for his arrest is his alleged link with the Maoists.¹³⁹

After the 2020 Delhi Riots, the Delhi Police seized the mobile phone of the AISA President Kawalpreet Kaur for investigation. In the seizure memo she was provided, a bunch of sections were charged, along with a few under the UAPA. Basically, the Delhi Police used the UAPA to now violate the privacy of individuals, seize their phones and basically do whatever they want under the pretext of an investigation.¹⁴⁰

In early 2020, a Kashmiri photojournalist who goes by the name Masrat Zahra, was arrested after she has posted some photos online which the police referred to as, "disturbing to communal harmony". While she was charged under Section 505 of the IPC, another bunch of sections were also added under the UAPA. A number of organizations have challenged this arrest, including press clubs, who say that this arrest is a blatant move of the police against the freedom of press.¹⁴¹

¹³⁸When Poetry is held Unlawful: A Case of Kabir Kala Manch, INDIA RESISTS, Apr. 23, 2015

April 23, 2015 <https://indiaresists.com/when-poetry-is-held-unlawful-a-case-of-kabir-kala-manch/>

¹³⁹ Devika Kohli, "Why Is The Government So Threatened By A Man Who Is 90% Disabled?", YKA, May 19, 2015. <https://www.youthkiawaaz.com/2015/05/gn-saibaba-arrest/>

¹⁴⁰AISA's Delhi head booked under UAPA by Crime Branch, mobile seized, INDIAN EXPRESS, Apr. 29, 2020. <https://www.newindianexpress.com/cities/delhi/2020/apr/29/aisas-delhi-head-booked-under-uapa-by-crime-branch-mobile-seized-2136830.html>

¹⁴¹First Post Staff, Masrat Zahra booked under UAPA: Kashmiri photojournalist's work focussed mostly on women, conflict reporting in Valley, FIRSTPOST, Apr. 20, 2020.

<https://www.firstpost.com/india/masrat-zahra-booked-under-uapa-kashmiri-photojournalists-work-focussed-mostly-on-women-conflict-reporting-in-valley-8278721.html>

In August of 2019, internet services and social media was brought to a complete halt in the Kashmir Valley, after the Central Government abrogated Article 370 of the Constitution of India, which provided special status of the state of Jammu and Kashmir. Post that, as of this day, only 2G services have been restored in Kashmir, and social media still remains banned. When some people in Kashmir actually tried accessing social media through a virtual private network (VPN), the police arrested them under the UAPA, and the already repealed Section 66A of the IT Act.¹⁴²

Given the monumental instances of blatant abuse of powers, arbitrary arrests, and disregard for human rights, it is only natural for one to be afraid of the UAPA, for it is not a law which should exist in a democratic society, but a weapon of oppression in hands of a mad government.

¹⁴² Vishnu gopinath, *Why Have People Using VPNs in J&K Been Booked Under UAPA?*, THE QUINT, Feb 18, 2020. <https://www.thequint.com/podcast/uapa-jammu-and-kashmir-vpn-social-media-illegal-unlawful-terror-geelani-video>

CHAPTER 6

INTERPRETATION AND ANALYSIS

6.1 Major Issues and Concerns: Impact of 2017 Judgement

The right to protect privacy of an individual is enumerated in the Universal Declaration of Human Rights, 1948 (UDHR) “*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, or to attacks upon his honor and reputation Everyone has the right to the protection of the law against such interference or attacks.*”¹⁴³ “The principle of Right to Privacy is also contained in International Covenant on Civil and Political Rights, 1976. The requirements under both the International treaty are that the state shall implement certain legislations to protect the right of privacy and attacks o reputation. As India is signatory to both the treaties, it is the mandate duty of India to pass such legislation but still India has not passed any separate and independent legislation dealing with the subject matter.”

“The Constitution of India does not explicitly guarantee fundamental right to Privacy though Judicial Activism has bought it within the realm of Fundamental rights.” Article 21 states “no person shall be deprived of his life or personal liberty except the procedures established by law.” “The Supreme Court of India deduced the Right to Privacy from Article 21 wherein the court held that personal liberty means life free from any encroachments that is unsustainable in law.” The court in a landmark judgment held that “the concept of liberty in Article 21 was comprehensive enough to include privacy and an unauthorized intrusion in to an individual’s home and thus disturbance caused violates his personal liberty.”¹⁴⁴ “In *People’s Union for Civil Liberties (PUCL) v Union of India*¹⁴⁵, the court explained right to privacy to be under Article 21 in consonance with Article 17 of International Covenant on Civil and Political Rights, 1968. The gross violations of the right to privacy

¹⁴³ Article 12 of Universal declaration of Human Rights, 1948 to which India is a signatory.

¹⁴⁴ *Kharak Singh vs. State of U.P.* AIR 1963 SC 1295.

¹⁴⁵ (1997) 1 SCC 301.

encouraged the Judiciary to take a pro-active role in protecting the right and providing the affected person adequate compensation and damages.”

In August 2017, the Supreme Court of India passed a judgment in the case of *Justice K S Puttuswamy vs Union of India*¹⁴⁶ (Supreme Court of India, WRIT PETITION (CIVIL) NO 494 OF 2012), in which fundamental rights, as provided in the Constitution of India, were interpreted to include the right to privacy. As a consequence of this judgment, the Government of India has an obligation both to ensure that its actions do not violate a citizen’s privacy and to ensure that such rights are not violated as a result of its inaction—including its failure to enact suitable legislation.

6.1.1. Data Protection and Aadhaar – The Biometric Authentication System

The case had its inception in 2012, when Justice K S Puttuswamy, a former Karnataka High Court judge, filed a petition before the Supreme Court questioning the validity of the “Aadhaar” project on grounds of, amongst other things, its transgression on the Indian citizen’s fundamental rights. The “Aadhaar” project is a 12-digit unique identification number that is issued to Indian citizens based on their biometric and demographic data. It is the largest biometric database in the world, with over 1.25 billion Indian citizens registered. The project raised several privacy concerns due to the almost mandatory requirement of enrolment and the lack of safeguards provided by the Government to protect the data collected. The argument made by the Government was that there was no constitutionally guaranteed right to privacy in India. Reliance was placed on two earlier Supreme Court judgments, *M P Sharma vs. Satish Chandra*¹⁴⁷ and *Kharak Singh vs. State of Uttar Pradesh*¹⁴⁸, which denied the existence of a constitutional right to privacy. Since these cases were decided by six- and eight-judge benches, respectively, the Supreme Court referred the matter to a constitutional bench of nine judges in 2015. Two

¹⁴⁶ AIR 2017 SC 4161.

¹⁴⁷ AIR 1954 SC 30.

¹⁴⁸ AIR 1963 SC 1295.

years later, this bench overruled the two cases to the extent that they decided that privacy is not a constitutionally guaranteed right.

“The Court decided that the protection of individual autonomy was a valid justification for the right to privacy, especially in the context of a global, information-based society. The judgment recognized the right of an individual to exercise control over his/her personal data. The Court opined that the ability of a person to control his/her own life would also encompass his/her right to control his/her existence on the internet. The Court further recognized the complexity involved in data protection and directed the Government to enact a comprehensive data protection law.”

Another important aspect of the Court’s ruling was the implicit recognition of a “right to be forgotten.” The Court stated as follows:

“People change and an individual should be able to determine the path of his life and not be stuck only on a path of which he/she treaded initially. An individual should have the capacity to change his/her beliefs and evolve as a person. Individuals should not live in fear that the views they expressed will forever be associated with them and thus refrain from expressing themselves.”

“Thus, the European Union Regulation of 2016 has recognized what has been termed as ‘the right to be forgotten’. This does not mean that all aspects of earlier existence are to be obliterated, as some may have a social ramification. If we were to recognize a similar right, it would only mean that an individual who is no longer desirous of his personal data to be processed or stored, should be able to remove it from the system where the personal data/ information is no longer necessary, relevant, or is incorrect and serves no legitimate interest. Such a right cannot be exercised where the information/ data is necessary, for exercising the right of freedom of expression and information, for compliance with legal obligations, for the performance of a task carried out in public interest, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defences of legal claims. Such justifications would be valid in all cases of breach of privacy, including breaches of data privacy.”

“These observations may increase the likelihood of the right to be forgotten or a similar right being incorporated into the forthcoming law. This right is distinct from the right to privacy which involves information that is not publicly known. It involves the removal of information that was publicly known at a certain time so that third parties cannot access it. Opinions about the right to be forgotten, which is a relatively new concept, differ significantly between the European Union, where it has more historical support, and the United States, where the right of free speech and the right to know have typically been favored over the deletion of truthfully published information.”

“If the right to be forgotten is codified into Indian law, search engines, social media platforms and media companies operating in India will be most affected. These entities may need to reconsider their internal processes and procedures for receiving and processing requests from members of the general public for the deletion of data. Google’s ongoing dispute with the French data protection agency, CNIL, illustrates how complex matters can become.” Now that the phrase “fake news” has become so common, the debate will become more urgent globally.

“With much appreciation and fame over the judgement which made Right to Privacy- a fundamental right’ by the Supreme Court, there still exists the issue of Aadhaar being valid or not which is still pending. Much controversy has lit upon the conflict of Aadhaar, specifically, The Aadhaar Act, 2016 and the Right to Privacy of every citizen of the country being violated through it. The problems with the Aadhaar Act, 2016 in concern to privacy are mainly comprised of two parts: firstly, Aadhaar Act making Aadhaar compulsory for every citizen and also making its compulsory linkage to other services, including PAN and phone numbers. It further makes an amendment to the Income Tax Act wherein for tax returns to be processed, one needs to link their Aadhaar number to their PAN.¹⁴⁹ A failure to do this could also lead to invalidity of the respective PAN. These legislations are a forced compulsion for the citizens to link their Aadhaar to these documents which is a problem as Aadhaar inherently requires a lot of personal and confidential information like

¹⁴⁹ Section 139 AA, Income Tax Act, 1961.

biometrics, fingerprints, etc. which connects to the second issue of data security.”

The Aadhaar Act, 2016 allows sharing of data under the Aadhaar numbers for the purposes of national security which is a vague and undefined term. Further, Aadhaar is applicable to commercial purposes as well and has the participation of private parties in its data access which leaves the citizens a huge risk of data leak given that there are no existing privacy laws in India. The present government wants the Aadhaar policy to continue and is gradually making Aadhaar mandatory for more documents, for e.g., driving license, which is in plan to also be mandatorily linked to Aadhaar.¹⁵⁰

The two core issues of the Aadhaar Act, its contradictions to the right to privacy and also its further consequences and misuses which have already started coming to existence. It further mentions the unique identification program in the United States (i.e, the Social Security Number) and its comparison to Aadhaar. It reflects upon how there is a much better possible regard to privacy when it comes to legislation which the intent of providing unique identity and for national security purposes. This links to the unnecessary essentials and requirements that are constantly being brought in by the present government and how it causes fundamental problems in the society.

6.1.2. The Linkage Problem

The Supreme Court in March, 2017 declared that Aadhaar cannot be made mandatory for availing governments’ schemes and subsidies.¹⁵¹ These include the PAN, Income Tax Filings, booking train tickets, etc., all of which now mandatorily require Aadhaar number for its processing. The BJP government, however, in its Financial Bill, 2017 added an amendment to the Income Tax Act, 1961. This amendment added a section which makes it compulsory for

¹⁵⁰ Kiran Rathee, “Govt plans to link driving licence with Aadhaar,” Business Standard, Sep 26, 2018. http://www.business-standard.com/article/economy-policy/govt-plans-to-link-driving-licence-with-aadhaar-117091600042_1.html.(visited on March 3, 2018).

¹⁵¹Editorial, “Supreme Court counters push for Aadhaar,” The Hindu, Mar 27, 2017. <http://www.thehindu.com/news/national/aadhaar-cannot-be-mandatory-for-welfare-schemes-supreme-court/article17671381.ece>.

citizens to link their Aadhaar numbers to their PAN for the purposes of Income Tax processes as well. The compulsory linkage further makes a PAN number invalid if not linked to the Aadhaar until a prescribed date by the Central Board of Direct Taxes (which presently is the 31st of December, 2017).

The legislation, by making such compulsory legislation, violated the Judiciary's decisions and observations. This was criticized by the Supreme Court as well because the compulsory linking of Aadhaar to PAN and further for the purposes of Income Tax returns makes it practically mandatory for any citizen to have an Aadhaar. This is in direct contradiction with the Supreme Court's intention to make Aadhaar voluntary. The dependence of Aadhaar on PAN and other services makes essential services and subsidies exclusive to only Aadhaar holders. A similar problem was identified by the Rajya Sabha before passing the Aadhaar Bill in 2016 where it opposed the Lok Sabha on several grounds one of them being the issue of Aadhaar being mandatory or not.¹⁵²

This recommendation was given during the due process of the bill and was at a later stage accepted by the Lok Sabha before enactment of the bill.¹⁵³ As a result of it, there exists section 7 in the Aadhaar Act, 2016 which states that any citizen who is not assigned an Aadhaar number will be provided with alternate and viable means of identification for delivery of a service, benefit or subsidy. The mandatory linking of PAN with Aadhaar having a further validity of tax returns is a clear violation of this section as it is ultimately being made voluntarily mandatory.

The conflict was taken up in the parliament and the Minister of Information and Broadcasting replied that the citizens not having Aadhaar shall be enrolled for one and an alternative method will be provided till an Aadhaar number is assigned to her. This statement directly negates the entire purpose of the optional clause in the Act. However, the Supreme Court in its judgement on

¹⁵² IANS, "*Rajya Sabha returns Aadhaar bill to Lok Sabha with amendments*," Hindustan Times, Mar 16, 2016. <http://www.hindustantimes.com/india/rajya-sabha-returns-aadhaar-bill-to-lok-sabha-with-amendments/story-uCVCaTLOVVyOVwrHqEuOSI.html>

¹⁵³ Editorial, "*Aadhaar bill is through after Opposition scores a few brownie points*," Indian Express, Mar 17, 2019. <http://indianexpress.com/article/india/india-news-india/rajya-sabha-returns-Aadhaar-bill-to-lok-sabha-with-oppn-amendments>.

the validity of Section 139AA, gave a partial satisfaction to both sides of the debate as it made the linkage compulsory only for existing Aadhaar holders.¹⁵⁴

6.1.3. Data Security and Infringements

An individual's unique identifiers such as fingerprint and retina scans are linked to his/her Aadhaar number. Authentication is carried out by comparing this information with the stored information of an Aadhaar cardholder. With the continuous increase in the number of facilities that mandatorily require Aadhaar information, the possibility of the misuse of Aadhaar information is also increasing, both by the state and private entities.

The Aadhaar Act has a clause that allows the Aadhaar information of an individual to be made available for state use in case of matters concerning "national security". This went through despite objections in the Rajya Sabha about the possible misuse of the term "national security".

Along with misuse by state, misuse by private agents is also a huge concern especially since the registration process for Aadhaar is carried out by private contractors who have access to all the incoming Aadhaar data. Identity theft then becomes very plausible since that information can be used to avail government-provided services in the name of the victim.

Another problem is the ease with which anyone can just walk into an Aadhaar registration center and enroll themselves. Immigrants, especially illegal immigrants can also enroll which becomes an obvious security threat. There have been allegations that this ease of enrollment has stemmed from political motivations of cashing in on the immigrant "vote bank".

One concern is related to data security. There are a number of organizations which require a customer to share his/her Aadhaar information as part of their "Know Your Customer" policy. There have been multiple instances where

¹⁵⁴ VS. Shivshankar, "Supreme Court Upholds Law to Link Aadhaar with PAN, Grants partial stay on Penal consequences," The Wire, July 1, 2017. Available at: <https://thewire.in/145800/sc-upholds-law-link-aadhaar-pan-grants-partial-stay/>. (visited on March 10, 2018).

customers' sensitive information has been leaked/hacked. This raises serious questions over the state of cyber-security technology in the country and the risk vs. reward of having a centralized database containing sensitive PII (Personally Identifiable Information)

6.1.4. Comparison to Social Security Number

fundamental rights directly link to the status of democracy in a country.

Aadhaar is not the only digital identification service run by a government. Other countries have also been running similar programs, like the Social Security Number in USA. However, there are some key differences which make Social Security Number a better alternative to Aadhaar in matters of security and hence privacy. First, the laws relating to security of personal information are much more stringent in USA as compared to India. Second, the use of Social Security Number is restricted only to State agencies which is in contrast to India, where the use of Aadhaar is continuously increasing in the private sector as well. Moreover, the design of the SSN system inherently reduces the risk of data theft by separating the storage of the number from other sensitive PII.

The push from the government in popularising the use of Aadhaar and linking it to other user information such as tax records through the Permanent Account Number are aimed at curbing fraud and other crimes. This gives rise to the age old security vs privacy debate. While security is a major concern, so is the privacy and hence freedom of the citizens of a country. If left unchecked, Aadhaar could become a tool for oppression by enabling individual surveillance in the hands of the government and a breeding ground for identity theft in unsecured data stores of private entities.

One way of controlling the blast radius from any security lax is to reduce the connectivity of Aadhaar to other sensitive PII and use it only as a means of authentication, much like the Social Security Number of the United States of America. Going forward, the burning question for us to answer is the compromise we are willing to make between the security and privacy of the

people of the biggest democracy in the world, a status which could come under serious threat if the privacy of citizens is ignored.

6.2. Negative and Positive Aspects

The Hon'ble Supreme Court of India in its 9-bench hearing and judgement has confirmed the Right to Privacy as a fundamental right. Even earlier it was a recognized right, but under common law. This makes it clear that Right to Privacy is a fundamental right. But it is not an absolute right. No Govt. including the freest of democracies, confer absolute rights on a citizen. It will come with its checks and balances, even within the scope of right to life and liberty. (For instance, it has to be subsumed under certain conditions of state security, public health and public morality).

There are few demerits, except perhaps in understanding and implementation both by the media and the legislature. A person's privacy is not an absolute. It needs to be defined according to the context. An individual has various levels of conduct. Roughly speaking:

- At the primary level is he/she with and within himself/herself. Like in food habits, dress, private behaviour, thoughts, etc.
- Within the close social unit like family and home.
- A little further out - to his/her specific community,
- Then his/her engagement with general society, state, and law systems.

To the extent that the use or misuse of this right is allowed or not, depends on the effect or repercussions of his/her conduct on those affected entities within which it functions (like home and family, community, general society). In short, your rights cannot transgress on the rights of others.

E.g.: Right to privacy in the bedroom is naturally an unambiguous right. But if it involves something like paedophilia, or bestiality or sadomasochism then it can definitely come under question.

Or, right to privacy on the Net is a fundamental right. But if it threatens the safety of someone or society or the security of the State, then it can be questioned.

So is the case with all fundamental rights. The context has to determine its application. And the context also has to decide whether it has been

transgressed or not. Also remember, the context can change with time and social ethos.

Now we will discuss the merits and demerits:

MERITS

- Know about them
- Emergency use
- Protect
- Identity
- Avoidance of copy
- Watchdog

DEMERITS

- Secure
- Leaks of the information
- Proper maintenance
- More technical knowledge
- Technology expertise
- Confinement/Slave
- Hit the freedom
- Fear

The above points have been applicable to nation Fundamental Rights of the “Right to Privacy”.

The Supreme Court cannot declare clear judgement regarding to the Aadhaar card from 2014 to present the action of card process on going till now. Every parliament rule, once bill has passed before that president have to discussed with Supreme Court of judges regarding to the bill or advice of laws doubts.

Afterwards, the Supreme Court has it says Ok, conformity of the bill is not inconsistency with our constitution then only can proceed further actions. On the ground, Supreme Court knows very well regarding to the Aadhaar card matters has collection of user biometric information. But, at initial stage the supreme court has given sanction to the plan of Aadhaar card. Hence, before final stage told that Right to privacy is Fundamental right. Aadhaar projects

had been spend more money for training of the staff and wastage of time, unnecessary actions were taken by the people.

Nation security = Right to privacy delete from FRs.

Person security = Right to privacy inserted into the FRs.

“For person, security important than the nation security, when person lives freely, the country running on smoothly.”

6.3. Need of Privacy Law In India

Technology has become the backbone of the way things work around us in this 21st century. That has brought a lot of data into our lives and this personal information is always out there and we are unaware of how this gets used. Birth dates, financial information, personal audio and video format data and everything related to our likes and dislikes is available to anyone tech savvy enough to get it. The same data is used by digital marketing companies to tailor make ads and target specific groups of people and on the other hand the same info if used with an ill intent can be used for harassment and ransom. Disappearing from the radar and living in a pre-historic time period is not a pragmatic approach and in today's worlds each transaction creates more digital data and increases our risk and exposure to cause harm to privacy. Time and again with the identification of bugs and scandals, personal info is leaked and is available to anyone who knows where to look for it.¹⁵⁵

Steps have been taken in the past to get privacy under the ambit of legislation. In 2009 BJD's Baijayant Panda had introduced a Bill in front of the Manmohan Singh led UPA-2. The party later drafted its own Privacy Bill and Panda had once again reintroduced a Bill to raise awareness around the issue. Panda's latest endeavour titled the Data(Privacy and Protection) Bill, 2017 has been presented before the House of Commons, Lok Sabha and is pending its approval. Its previous iteration was called the Prevention of Unsolicited Telephonic Calls and Protection of Privacy Bill. The crux of this bill was to prevent the invasion of privacy by call centres who try to forward their business interests to unassuming common public. The 2009 bill was a private member bill and it defined privacy stating that, “every person shall have the

¹⁵⁵ Importance of data protection, <http://www.bgr.in/features/privacy-why-it-is-important-for-users-to-protect-their-own-data/> (visited on March 22, 2018)

right to privacy and freedom to lead and enjoy his life without any unwarranted infringement.”

Adding to the list of vocal politicians on the need of privacy laws is Rajya Sabha MP Rajeev Chandrasekhar who had proposed a privacy bill in 2010. BJP Lok Sabha ,MP Om Prakash Yadav and Trinamool Congress Rajya Sabha MP Vivek Gupta had also introduced two bills in 2016 but none of these efforts have received a thumbs up from the Parliament.

Panda’s latest iteration of the bill points towards the consent aspect of online data handling and privacy. It states that the person shall have the sole right and final right to modify or remove personal data from any online database, present in any part of the country, public or private. Regarding the cases that will be exceptions to the bill, the resolution is proposed on a case by case basis.¹⁵⁶

6.3.1. Necessity of Legislation of Right to Data Privacy

Ever since the advent of the telephonic and information age in the late 20th century various legislations have been put in place which cover different aspects related to Telephones, Cellular data and IT. These legislations do provide guidelines around the issues pertaining to the mentioned industries but leaves a lot to be desired in the case of Right to data Privacy. Also the precedent set by Jurisprudence in our country does not inspire a lot of confidence as the interpretation is highly subjective. Cases have been there where a bench has voiced differing opinions in important cases clearly demonstrating the divergence in understanding. Summing up these issues there is a rising consensus amongst the Judiciary to put a new legislation in place to provide Rights to the citizens of this country to protect their identity online.

The laws which are already in place fall short in providing any security or investigation to the victims of the data attacks on an international scale, primarily in Nigeria and China. The economic cost of such attacks is

¹⁵⁶ Right to privacy: fundamental right,
<https://www.indiatoday.in/india/story/right-to-privacy-fundamental-right-parliament-1031136-2017-08-24>
(visited on April 17, 2018)

extremely high and several Anti-Virus companies are predicting the rate of such events to sharply rise in the coming future. Sony, Snapchat, Yahoo, Apple are just some of the big international players who have been targeted for user data. Besides our own nation has faced multiple such incidents, Zomato, Reliance Jio and Aadhar are to name a few.

The Government has risen to the need of the hour and has proposed to enact specific legislations on Privacy. The proposed bill on being implemented will empower the user by overriding the IT Rules and giving an individual's privacy back. Cases pertaining to protection of national security, national integrity or sovereignty, public order and prevention of crime will be an exception to the law. The following are the reasons for the delay in implement the Privacy Bill¹⁵⁷

- “A disagreement between the judiciary and intelligence agencies over whether or not the agencies ought to be under the scrutiny of a competent court with respect to interception of personal data when they deem it necessary.”
- “A debate over the extension of protection granted by the legislation to all residents’ of the country (as opposed to only the citizens).”

The latest draft of the Bill is being discussed behind closed doors but it is supposed to be more transparent than the IT Rules. It specifically states that the personal data should be treated in fair and lawful manner.¹⁵⁸ Authorities involved in handling to such sensitive personal data will be under obligation to treat it as confidential and in no way share it with any third party. The data controller and processor must strive to maintain the quality and accuracy of the data and prevent it from destruction.¹⁵⁹ The Bill also puts the authority of Intelligence agencies under check and states that the said agencies will have to minimize the number of people in their organization to whom the data will be made available and the extent to which such data can be copied.

¹⁵⁷ Data protection laws and regulations 2020
<http://www.iclg.co.uk/practice-areas/data-protection/data-protection2016/india> (

¹⁵⁸ Privacy Bill. Sec. 9, Sec. 10

¹⁵⁹ Privacy Bill. Sec. 15

Data along with the exposure to fraud and privacy invasion also poses the threat of surveillance. To protect the interests of the citizens Chapter IV of the Privacy bill handles the issues around the Data Protection authority. It outlines the process of appointment of key chair people and their removal, functions of such authority, powers and the powers relating to enquiries.

6.3.2. Necessity of Legislation of Right to Data Privacy (2017)

Orissa MP Baijayant Panda has introduced the Data Privacy and Protection Bill in the parliament as a private bill with the intention to raise awareness around the issue of the right to data privacy of individuals in the digital age. A guiding force behind this Bill was the 9 judge constitutional bench in the Supreme Court looking into the right of privacy and by extension Aadhar. The Bill narrows down the issue to data privacy alone but the bench is looking into privacy as a whole.

6.3.3. Precedents and History

Historically the first nation to introduce guidelines around legal Data Protection was US, where they introduced the US Privacy Act 1974. Since then more than 100 countries have integrated rules regarding data Privacy in their legislation as reported by Privacy International. Data Protection is a legal right in the UK and it is under review to align with that of the EU which in itself is said to have one of the most comprehensive rules in this field.

In our own nation there have been multiple instances where the judiciary has given judgements based on different interpretations of the concept, indicating on one hand that the matter is subject to national security consideration and yet on the other hand begs to draft some solid guidelines to eliminate any doubt. The rulings were the basis of the IT Act of 2002, Indian Telegraph Act of 1885 which provided for extraction of data without any consent. Under these cases the only way to protect an individual's interest was only after the approval of a senior officer as laid down by the respective acts and the case shall have to be in the interest of national security or greater public good. Clearly these acts have an out-dated style and cannot keep up with the modern day advancements in the cyber data breach incidents. They also do not hold up to the standard of

getting individual consent before processing any personal data. The most the IT ACT(2008 amendment) provide is penalties for offender and protection against breach of sensitive data privacy but beyond that it does not crystallise the process to be followed to collect, store and process data to name a few.

6.3.4. Objectives of the Proposed Bill

The Bill aims to constitute a Data Privacy Authority at a national level which will strive to protect the digital privacy of its citizens. The gargantuan amount of data produced everyday on the social media platforms exposes a lot of personal data and till date they have been protected by the Privacy agreements signed in accordance to the US law. There have been a lot of data breaches in the past of such US based companies and then grievance redressal in such cases becomes a herculean task. Hence the authority will strive to define the extent of privacy and establish methods to identify data leakages, protection and monitoring mechanisms.

i. Establishing the Right to Privacy

Consent will be the core value of the Bill, it will give that power in the hands of the citizen, the way it should be and is followed in other countries. It will also make provisions to determine the nature of data stored, altering or rectifying existing data. It also irons out the problem of the uniform storage of data compatible to universal standards and secure enough to be transmitted amongst the service providers without any threat.

Features

- Profiling of individuals and setting up data processing is a welcome addition with the Bill
- Elimination of interpretation by clearly setting down definitions helps maintaining the balance from tipping into the hands of the state which oftentimes can use sweeping generalizations in its own favour

- For example, Section 66A of the Information Technology Act, which was repealed by the Supreme Court in 2015.
- Empowers the individual by following a rights based approach and mandating consent for collection and processing data
- It also gives the power to alter or delete any information from a public or private database to the individual itself
- Moreover the exceptions against this right is supposed to be handled on a case by case consideration
- The bill allows for grievance redressal through the appointment of an Information assurance officer with an arrangement for offer to the Data Privacy and Protection Authority (DPPA)¹⁶⁰
- Right to Privacy is proposed to be added to the Fundamental rights to the citizens of our country
- Ensures that the data collectors and data processors collect and process data in a predefined law abiding manner
- Ensures the security of the data in transit by setting up obligation on the data intermediaries
- Surveillance by the state will be limited by the guidelines mentioned in the interest of Security
- Authorises the Data Privacy and Protection Authority to raise concerns by the individual against the government or independent institutions and get compensation for losses and even imprisonment for the guilty Provides the option for impact assessment and consultation by the DPPA.

ii. Standard Operating Procedure For Data Collection, Transfer And Storage

Data storage providers land with the responsibility to receive consent from the

¹⁶⁰ *Ibid*

user regarding usage of their data as well as of ensuring secure data storage. Well outlined provisions have been made for the disabled and minors. The bill drafts a time framework during which data can be stored.

iii. National Security Implications

The bill integrates the national security aspect in line with the existing bill but additionally provides for surveillance of individuals and groups under investigation of activities which could cause national harm or threat of any sort.

iv. Safeguards & Constitutional Authority

The bill has come up with its own set of penalties and punishments for offences related to the invasion of data privacy, hacks to confidential data etc. It shall override the already setup penal conditions under the IT Act and the Telecom Regulatory Authority of India Act.¹⁶¹

v. Regulatory Structure proposed by the bill

The bill proposes the setting up of a Data Privacy and Protection Authority (DPPA) which will have members from both the legal and technical community, preferably equal in count, which will undertake the cases brought under its purview. They will also be empowered to conduct inspections of data controllers and processors to ensure no malpractice happens. They can also have consultations to improve the data security and privacy to meet the changing needs of the day. This Bill has raised a lot of discussion around the topic and though in the current scenario the chances of it passing are grim due to political issues, it still sets the right precedent as and when such a bill gets passed.

The Bill aims to give the citizens the Right to Privacy as a statutory right under Section 4 of the Constitution but this right is only pursuant to Articles 19 and Article 21.¹⁶²

¹⁶¹ The Data (Privacy And Protection) Bill, 2017
<http://www.thedialogue.co/analysis-draft-data-privacy-protection-bill-2017/>

¹⁶² *Ibid.*

6.4. Philosophy and Importance of Mass Surveillance

There is a very common sentiment. In this debate even with people who are comfortable in mass surveillance, They say there is no real harm that comes from this large scale of mass Surveillance invasion because only people who are engaged in bad acts have a reason to want to hide and to care about their privacy. this world view is implicitly grounded in the proposition that there are two kinds of people in the world: good people and bad people. Bad people are those who engage in terrorist attacks and violent criminalities. They have reason to hide, have reason to care about their privacy. By contrast, the good people are the people who go to work, come home, watch television , and spend time with family. They use internet not for planning bombing attacks, rather they use to exchange mails, share recipe and read news and these people find nothing wrong in surveillance they do not have any reason to fear the government monitoring them

The people who are saying it, are engaged in a very extreme act of self-depreciation, what they are really saying is, “I have agreed to make myself such a harmless and unthreatening and uninteresting person that I actually do not fear having the government know what it is that I am doing.” This mind-set has found what I think is its purest expression in an 2009 Interview with the long-time CEO of Google - Eric schmidh, who when asked about all the different ways in which his company is causing invasion of privacy for hundreds and millions of people around the world, he said, “*if you are doing something you don’t want other people to know, maybe you shouldn’t be doing it in the first place.*”¹⁶³ Now, there’s all kinds of things to be said about this mentality, the first of which is that the people who say that privacy isn’t really important, they don’t actually believe it and the way you know that they don’t actually believe it , is it while they say their words that privacy actually doesn’t matter but their action takes all kinds of steps to safeguard their privacy. They put passwords on their e-mails, social media accounts. They put

¹⁶³ *Google CEO On Privacy: ‘If You Have Something You Don’t Want Anyone To Know, Maybe You Shouldn’t Be Doing It*, HUFFPOST, Mar. 18, 2010.
https://www.huffpost.com/entry/google-ceo-on-privacy-if_n_383105

locks under their bathrooms, bedroom doors all steps to prevent people from entering what they call their privacy and private space.

The very same Eric schmidt ,the CEO of Google, ordered his employees at Google to cease speaking with an online internet magazine- CNET,after CNET published an article full of personal, private information about Eric schmidt, which it exclusively obtained from Google searches and using other Google products, this same division could be seen with CEO of Facebook, Mark Zuckerberg who in an infamous interview in 2010 - pronounced that, “*privacy is no longer include social norm*”¹⁶⁴, in 2014 MARK Zuckerberg and his wife purchased a house along with all 4 adjacent houses in Paulo Alto for 30 million \$ so that they can enjoy their privacy

And to prevent other people from monitoring what they do in their personal lives. Over the last few months while researching about the said topic, everybody who mentioned that he or she doesn't worry about invasion of privacy because they don't have anything to hide , but when asked in return to take out a pen and give their email addresses and passwords of all email accounts not just the nice respectable work emails in their name but all of them, because what harm would there be in just wanting to scroll through what they're doing online, read through what I want to read and publish what I find interesting after all if they are doing nothing wrong , they should have nothing to hide, not a single person in reality takes up on that offer.- There is a reason for that ,that us as human beings even though which of us in words do not oppose surveillance , we Instinctively understand the profound importance of it. It is true that human beings are social animals ,which means that we have a need for other people to know what we are doing , and saying and thinking, which is why while we voluntarily publish information about ourselves online, but its equally essential to feel what it means to be a free and fulfilled human being is to have a place where we can go and be free from the judgemental eyes of the people, there is a reason why we seek that out and the reason is that all of us not just terrorists and criminals but all of us have thing to hide.

¹⁶⁴ Emma Barnette, *Facebook's Mark Zuckerberg says privacy is no longer a 'social norm* , THE TELEGRAPH , Jan.11 , 2010
<https://www.telegraph.co.uk/technology/facebook/6966628/Facebooks-Mark-Zuckerberg-says-privacy-is-no-longer-a-social-norm.html>

There are all sorts of things that we do or think or tell our physician or lawyer or our psychologist or our spouse or our best friend that we would be mortified for the rest of the world to learn, we make judgements every single day about the kind of the things that we say or think or do or are willing to have other people know and the kind of things we say or think or do which we don't want anyone to know about people can very easily in words claim that they don't value their privacy but their actions after negate the authenticity of that being.

There is a reason why privacy is so craved universally and distinctively, it is not just reflexive thing like drinking water and breathing air, the reason is that when we are in a state where we can be monitored and where we can be watched, our behaviour changes dramatically, the range of behavioural options that we consider, when we think we are being watched on surveillance is reduce. This is just a fact of human nature that has been recognised in social science and literature and in religion and other virtually in every field and discipline. There are dozens of psychological studies which prove that when somebody knows that they are being watched, or might be watched, the behaviour they engage in are usually more conformist and compliant. Human shame is a very powerful motivator and as is the desire to avoid it and that is the reason that when people are in a state of being watched, they make decisions not that are the by-products of their own agency but out of the expectation that the others have of them and the mandates of other societal orthodox. this realisation was exploited most powerfully for the pragmatic ends by 18th century philosopher Jeremy Bentham, who set out to resolve an important problems ushered by in industrial age, where for the first time the institutions had become so large and centralized that they were no longer to control or monitor individual members and, the solution he devised was an architectural design, originally intended to be implemented in the prisons that he called "*panopticon*"

"The primary attribute of which was construction of an enormous tower in the centre of the institution where whoever controlled the institution could at any moment watch any of the inmates, although they could not watch all of them at all times and crucial to this design was that the inmates could not see into the panopticon tower so that they never knew if they are being watched or even

when. And what made him so excited about this discovery was that the prisoners would have to assume that they are being watched at any given movement which would be the ultimate enforcer for obedience and compliance.” The 20th century French philosopher ‘Michel Foucault’ realised that the model could be used not only for prisons, but every institution that seeks the control of human behaviour - schools, hospitals, factories, workplaces and what he said that, “This framework discovered by the Bentham is the key means of societal control from modern western societies which no longer need the older overt weapons of tyranny - punishing or imprisoning or killing the dissidents , or legally compelling because mass surveillance create a prison in the mind that is a much more subtle and much more effective means of fostering compliance with social norms over social orthodoxy and much more effective than crude force can ever be.”

The most iconic work of literature about surveillance and privacy is George Orwell’s novel 1984. Whenever it is brought upon in a debate about surveillance, people instantaneously dismiss it as inapplicable. The conversation generally starts with, “*well in 1984 there were monitors in people's home they were being watched at every given moment and that has nothing to do with the surveillance that we face.*”¹⁶⁵

That is an actual fundamental Misapprehension of the warnings that Orwell issued in 1984. The warning that he was issuing was about a surveillance state not that monitored everybody at all times, but where people were aware that they can be monitored at any given moment.

Here is how Orwell’s narrator, Winston Smith describes the surveillance system that they faced that, “*There was, of course, no way of knowing whether you were being watched at any given moment.*” He went on to say, “*At any rate they could plug in your wire whenever they wanted to You had to live, did live, from habit that became instinct, in the assumption that every sound that*

¹⁶⁵ Robert Draper, *They Are Watching You—and Everything Else on the Planet*, NATIONAL GEOGRAPHIC MAGAZINE, Feb 2018.

you made was overheard and except in the darkness every movement scrutinized.”¹⁶⁶

The Abrahamic religions similarly posit that there is an invisible, all knowing authority who, because of its omniscience, always watches whatever you are doing, which means you never have a private moment, the ultimate for enforcing obedience to its dictates. What all of these seemingly disparate works recognize, the conclusion that they all reach, is that the society in which people can be monitored at all times is a society that breeds conformity and obedience and submission, which is why every tyrant, the most overt to the most subtle, craves that system. Conversely, and even more importantly, it is a realm of privacy, the ability to go somewhere where we can think and reason and interact and speak without the judgemental eyes of others being cast upon us, in which creativity and exploration and dissent exclusively reside, and that is the reason why when we allow a society to exist in which we're subject to constant monitoring, we allow the essence of human freedom to be severely crippled.” In conclusion to this, the last point that has been observed about this mind-set, “The idea that only people who are doing something wrong have things to hide and therefore reasons to care about privacy, is that it entrenches two very destructive messages, two destructive lessons, the first of which is that the only people who care about privacy, the only people who will seek out privacy, are by definition bad people. This is a conclusion that we should have all kinds of reasons for avoiding, the most important of which is that when you say, “somebody is doing bad things,” you probably mean things like plotting a terrorist attack or engaging in violent criminality, a much narrower conception of what people who wield power mean when they say, “doing bad things.” for them, “doing bad things” typically means doing something that poses meaningful challenges to the exercise of our own power, the other really destructive and even more insidious lesson that comes from accepting this mind set is there's an implicit bargain that people who accept this mind set have accepted, and that bargain is that, “if you're willing to render yourself sufficiently harmless, sufficiently unthreatening to those who wield political power, then and then can you be free of the dangers of surveillance. It's only

¹⁶⁶ GEORGE ORWELL, 1984, (Sevker & Warburg) (1948)

those who are dissidents, who challenge power, who have something to worry about.”

“There are all kinds of reasons why we should want to avoid that lesson as well. You may be a person who, right now, doesn’t want to engage in that behaviour, but at some point in future you might. Even if you're somebody who decides that you never want to, the fact that there are other people who are willing to and able to resist and be adversarial to those in power - dissidents and journalists and activists and a whole range of others- is something that brings us all collective good that we should want to preserve. Equally critical is that the measure of how free a society is not how it treats its good, obedient, compliant citizens, but how it treats its dissidents and those who resist orthodoxy. The most important reason is that a system of mass surveillance suppresses our own freedom in all sorts of ways.” It renders off-limits all kinds of behavioural choices without our even knowing that it’s happened. The renowned socialist activist Rosa Luxemburg once said, “*He who does not move, does not notice his chains.*” “We can try and render the chains of mass surveillance invisible or undetectable, but the constraints that it imposes on us do not become any less potent.”

6.5. WHY PRIVACY? Indian Privacy Code 2018

Cambridge analytica, NAMO app, Paytm, adhar card, there is one thing very common among the controversies that has risen around all these apps in recent times. It is alleged that all these apps are trying to steal the personal data. So what is there in the that data that is worth stealing? What is the solution?

The controversy of cambridge analytica shook the Governments across the entire world. And since then, they have started making laws related to data protection and data privacy..

In 2018, In the state of Uttar Pradesh, potato farmers wanted to protest against the controversy which was there at that time due to the intermediaries in the business and low price at which they had to sell their product. The Farmers allegedly dumped potatoes outside the houses of the government officials.

Uttar Pradesh government got agitated with this and to catch the people responsible who exactly had done this, they tapped more than ten thousand phone calls. It would be some 10-20 people who must have dumped it, but, extra nine thousand nine hundred and eighty people's phone calls got taped. All the conversations that must've happened between the innumerable people got taped.¹⁶⁷

In another case, in Andhra Pradesh, a government website publicly displayed people's private information. They did not do it intentionally but since the website was so insecure that it happened anyway. This data was about a government medical store and the information about the people, their phone number and the details of the medicine purchased by them. Stringent data protection laws must be made where the people carrying sensitive data can be held accountable for such mishaps and there is proper management system if and when such leak of data crisis arises.

Furthermore, Privacy is a fundamental right just like the other rights in the constitution, this was then declared by the SC, After this decision by the SC, the government was compelled to take the action against it. The government's ministry of information technology had appointed an expert panel to draft the new data protection law, this expert panel was headed by the supreme court's judge B.N shri krishna. They were given a task to prepare a draft based on which a law could be made. Considering the draft inadequate, a group of common people, from every walk of life, the experts and organisations got together, who felt the need to step forward and take an initiative and took it upon themselves to form a strong policy draft to be presented in the parliament. In this group there were 13 different groups which included, legal experts, policy analysts and lawyers. Together they all prepared a draft for data privacy which they have named as Indian privacy code 2018. This draft was supposed to be a modern bill, which means that if the government wants to make this as law then they will have to bring this in the parliament and pass this to make a strong data protection law.

¹⁶⁷ *Potatoes hurled outside UP CM Yogi Adityanath's residence, other prominent places in Lucknow; here's why*, FINANCIAL EXPRESS, Jun. 6, 2018.
<https://www.financialexpress.com/india-news/potatoes-hurled-outside-up-cm-yogi-adityanaths-residence-other-prominent-places-in-lucknow-heres-why/1004545/>

The unique thing about this bill was that those people had brought the entire draft in front of the common people. Their website was saveourprivacy.in. Where anybody could read their 20-25 pages draft line by line in this website and even give the suggestion.

A person could highlight any part, line and annotate it to write their comments too. It was the first time such an open law has been kept for the public to analyse.

A brief summary of the bill to understand why was this so important for everybody and why it's important to defend this fundamental right to privacy. As a summary they had given seven principles of privacy :

Principle 1 says individual rights are at the centre of privacy. That means that an individual needs privacy the most. A government or a company does not need privacy, in fact the more they are transparent, the more it is beneficial for the country

Second principle says that data protection law must move ahead with the technology. There should be exceptions in it but they should be clearly defined and limited, it should not happen that the law gets pressurised under the exceptions.

Third principle says that a new strong and independent body should be made named privacy commission. This commission will look after the privacy related matter and will see how well is this law being implemented. It will have investigative powers and will also see that the law is not getting outdated and is getting changed with time.

Fourth principle stated that the government should respect the user's privacy. That a government should respect an individual's right. This new commission will have its authority valid on the government as well

Fifth principle says that the surveillance should also be considered in the privacy. Phone tapping by the government or illegal raid in people's house also comes under infringement of privacy

Sixth principle is that the right to information law should also be empowered here and it should be strengthened and protected

International protections and harmonisation to protect the open internet must be incorporated. That means if there is any good law being made in the world, it should be adopted and get inspired to implement them here. Like recently a very strong data protection law was introduced in Europe called GDPR.

Indian privacy code has taken a lot of inspiration from GDPR, few things are used as it is. And few areas adopted as per the Indian standards.

Like in GDPR, if you open any website in Europe, then the website will have to ask you whether they can track you or not? You can either accept or decline. so, this was a term in GDPR , now Indian privacy code adapted it with a straight ahead of just accept and decline as majority of the country's population is not well read.

These 7 principles are basically a summary of what is there in the Indian privacy code, and why is this necessary and it's so important there are many reasons for it.

The earlier stated two examples of Uttar Pradesh and Andhra Pradesh were mentioned to bring into perspective that how government misuses its power to carry out surveillances and that in Andhra Pradesh how data when leaked by mistake also has severe consequences if fallen in the wrong hands, now let's move a step ahead and see how is data which is available publicly can be misused in a dangerous way example of cambridge analytica and how voting manipulation can be done using your data seems like a poster case for everything which is wrong with the system, the ignorance and non-stringent data protection laws.

Cambridge analytica used to use Facebook likes to spread propaganda for political parties, by understanding pattern behaviours and likes of the individuals and accordingly targeting them with spreading selective propaganda using the things people enjoy, this is nothing but manipulation.

Returning back to the topic of the code, it is also mentioned in the Indian privacy code 2018 that if government invades privacy then it should have a legitimate state purpose and that state purpose should be proportional to the extent of privacy being invaded. So if there is a small crime like someone has slapped somebody then 10,000 people's phone getting tapped like in the potato case is infringement of privacy by using arbitrary powers, So proportional representation should be there here.

6.6. Brief Analysis On How National Security Agencies Pierces The Right To Privacy Of The Citizens Under The Excuse Of National Security.

Leaving digital footprints

In the digital age that we have stepped in, the most valuable commodity is data. Data today decides who will have money, power and influence. Majority of the multibillion dollar companies like Facebook and Google are data based. They not only process and displace data, they also store and monitor data.

*“It was recently exposed that the social media giants and search engines like Facebook and Google sell data for revenue to private players”.*¹⁶⁸

While this is very alarming, there is still the relief for those who have nothing to do with the internet, the people in the villages who are not tech savvy. However, the real threat to the privacy of the individuals comes from the most unexpected source: The Government. The last decade stands witness to the various incidents of not only agencies snooping data under the government's nose but incidents of government ordered breach of data privacy.

The governments of the world have always been active when it comes to snooping data, the digital age just made it a lot easier. In the times of landline phones, there were phone tapping, which still exists in many countries. There are now more sophisticated ways to communicate and therefore better ways for the government to snoop.

¹⁶⁸ *Facebook's data-sharing deals exposed*, BBC (Nov 05, 2019 7:20) <https://www.bbc.com/news/technology-46618582>

Today the reality is far grimmer than we can imagine. It is not just our emails and messages that the government sees, it reaches far beyond our wildest imaginations. The data which we might think of as useless apparently is very useful to the government. *“Our complete life including the TV programs we watch, the restaurants we visit and even the sidewalks we prefer is being watched by the governments of the world”*¹⁶⁹.

The entire list is way too lengthy to describe but certain moves that are monitored by the governments of the world are -

1. License plates via reader traffic cameras.
2. Sidewalk and public space movement by cameras.
3. Movement via public transportation.
4. Use of Credit and Loyalty cards
5. All data and use activity on phone.
6. TV history
7. Computer activity
8. Emails

Earlier in this decade, the news of the US Government spying on its citizens and beyond took the internet by storm. It was revealed by a former Central Intelligence Agency employee Edward Snowden. The revelations told the world that after 9/11, the government has snooped on each and every activity of not only its citizens but also people from different countries. From snooping into emails to even hacking the webcams of the computers. *“The agencies were not only monitoring this data but also storing it. This was a clear and gross violation of the right to privacy of the citizens of the world and especially American citizens.*

*The snooping had deeper roots than we can comprehend and it was covered by The Guardian”*¹⁷⁰.

It seemed scary at that time but we Indians kept calm, however, that did not last for long when we came across the snooping that our government has been doing on all of us.

¹⁶⁹ Sara Schwartz, *9 Ways You're Being Spied On Every Day*, HUFFPOST (Nov 5, 2019, 7:21) https://www.huffpost.com/entry/government-surveillance_n_5084623

¹⁷⁰ *NSA Files decoded*, The Guardian, (Nov 5, 2019) <https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/2>

“It may come as a surprise to most people but as of December 2018, a few government agencies have been empowered, via a notification in the official gazette, to snoop on any computer in the country. This order which came from the Government of India left everyone in shock”¹⁷¹.

The following agencies are named in the notification:

- *“Intelligence Bureau”*
- *“Narcotics Control Bureau”*
- *“Enforcement Directorate”*
- *“Central board of Direct Taxes”*
- *“Directorate of Revenue Intelligence”*
- *“Central Bureau of Investigation”*
- *“National Investigation Agency”*
- *“Cabinet Secretariat (RAW)”*
- *“Directorate of Signal Intelligence”*
- *“Commissioner of Police, Delhi”*

These have been named and authorized to snoop on anybody and everybody in the country. The government says that this has been done to ensure safety for the citizens and weed out the dangerous elements of society, foreign infiltrators, spies and other threats to the national security. There is a belief that there can be no prevention without intelligence and no intelligence without snooping. The goal to protect the people needs to have some powers which may infringe some rights of the citizens. Almost all the countries in the world which have a functioning intelligence system run surveillance over everyone in their vicinity and beyond. There can be no peace without apprehending dangers before they materialize and it will require snooping.

However, this snooping often leaves the boundaries of security and becomes the tool at the hands of the government to use it for political gains. A complete check on the movement and activity of every citizen, every opponent and every officer in the country completely nullifies the right to privacy enshrined in the Constitution itself.

¹⁷¹ 10 central agencies can now snoop on "any" computer they want, ET Times, (Dec 21, 2018, 01.30 PM) <https://economictimes.indiatimes.com/news/politics-and-nation/10-central-agencies-can-now-snoop-on-any-computer-they-want/articleshow/67188875>

The most recent blow to the government on snooping came from the Bombay high court this month where the two judge bench nixes the government on phone tapping and clearly stated that, “*unless they meet the three criteria set by the nine judge bench in Puttuswamy case, the government cannot do phone tapping. The records were ordered to be destroyed*”¹⁷².

Recent Judgment

As we have already established that the right to privacy is a fundamental right and infringing the right may be gross violation of the same which is concluded in a recent judgment. The division bench of justice Kanjit More and justice N.J. Jamadar : Bombay High Court, granted relief to a 54 years old businessman based in Mumbai and quashed three separate orders by ministry of home affairs which allowed central bureau of investigation to intercept phone calls of the petitioner in the case of bribery which involved a public sector official working in a public bank.

According to CBI the petitioner gave a bribe of rs10 lakh to the said bank official for credit related favors.

In three separate orders dated October 29,2009, December 18, 2009 and February 24,2010, phone tapping or interception of telephone calls of the petitioner was allowed, soon after CBI registered an FIR against the petitioner on April 11, 2011

The contention of the petitioner was that this was a gross violation of his fundamental rights guaranteed under part III of the constitution, and the action taken was ultra vires of section 5(2) of the Indian telegraph act, 1885.

Senior advocates of eminence, Vikram Nankani along with Dr. Sujay Kantawalla appeared for the petitioner in the case. They referred to the landmark judgment given by Supreme Court in 2017 through a nine-judge constitution bench’s decision in K.S. Puttaswamy v. Union of India and the decision given in People’s Union for Civil Liberties (PUCL) v. Union of India

Arguments: that the alleged illegally intercepted the telephonic conversation.

¹⁷² Swati Deshpande, *Bombay high court nixes government's phone-tap orders as they 'violate right to privacy'* TIMES OF INDIA (Oct 23, 2019, 9:13)<https://timesofindia.indiatimes.com/india/bombay-high-court-nixes-governments-phone-tap-orders-as-they-violate-right-to-privacy/articleshow/71713403.cms>

That the recordings contained in the charge sheet and any material that was acquired on the basis of such illegally intercepted telephonic recordings should not be admissible.

That it would be violation of the provision given under the Indian telegraph Act, under section 5(2) which states that such interceptions can take place only on the occurrence of any of the two events, first in the case of some public emergency, or in the interest of the public safety

The PUCL case was affirmed by Supreme courts constitution bench in the landmark judgment of KS Puttuswamy. In the same case, another decision of the Supreme Court was referred to, which was “*R.M. Malkani v. State of Maharashtra*”¹⁷³ . The bench also scrutinized test to ensure that right to privacy of an individual is not infringed upon principles of legitimacy and proportionality.

The test suggests that it is necessary and how to limit the discretion of the state because of the various concerns which were raised and expressed on the behalf of the petitioner arising from the mere possibility that the state is infringing the right to privacy. The following are the key test elements –

- The action must be backed by the law, which means that there should be a sanction by law.
- The action which is proposed must hold some importance and must be of absolute necessity in the democratic society and must be for a legitimate reason or aim.
- The extent of such interference must be proportionate to the extent of need for such interference.
- In case of such interferences, there must be procedural guarantees.

Justice More who authored the judgment noted- "*We are of the view that as per Section 5(2) of the Act, an order for interception can be issued on either the occurrence of any public emergency or in the interest of the public safety. The impugned three interception orders were issued allegedly for the reason of public safety. As held in PUCL , unless a public emergency has occurred or*

¹⁷³ R.M. Malkani v. State of Maharashtra, 1973 AIR 157

the interest of public safety demands, the authorities have no jurisdiction to exercise the powers under the said section.” “The expression Public Safety as held in PUCL means the state or condition of freedom from danger or risk for the people at large. When either of two conditions are not in existence, it was impermissible to take resort to telephone tapping”¹⁷⁴

While giving the judgment, it was clearly stated that if the direction given by the supreme court in the PUCL case which was then approved and re-enforced in the K.T. Puttaswamy case regarding illegally intercepted messages pursuant to an order having no sanction of law are openly disregarded then they will amount to nothing else but a serious case of contempt for law, that too in the matters involving breach of fundamental right of privacy under Article 21 the constitution of India. Fundamental rights if put outside the scope of protection, in the administration of criminal law, the concept that the ends would justify the means would amount to openly stating that the Government authorities may violate any directions Apex Court or mandatory statutory rules in order to procure evidence against the citizens. If the situation is observed closely, it is a gross violation of life and liberty of the citizens, it would do nothing but would lead to manifest arbitrariness and would promote the minimal regard to the procedure and fundamental rights of the citizens, and the laws laid down by the supreme court of India.

“The Supreme Court deliberated on the contours of “Right to Privacy”. A critique of the development of law pithily puts it thus: All nine judges unanimously held that the right to privacy was an essential element of dignity and liberty; and despite holding that the right was not absolute, couched the same in expensive terms as is beautifully encapsulated in the following passage from the opinion of Justice DY Chandrachud (speaking for four out of the nine Judges): “Privacy lies across the spectrum of protected freedoms. The

¹⁷⁴ Vinit Kumar and ors v. Central Bureau of Investigation

guarantee of equality is a guarantee against arbitrary state action. It prevents the state from discriminating between individuals”¹⁷⁵

6.7. Application Ban

Amidst rising tensions with Chinese counterparts, the Indian government through its Ministry of Electronics and Information Technology has recently blocked the availability of 59 Chinese applications in India. Apps affected by this ban include social media apps like TikTok, Helo and WeChat; and also other highly-used apps like ShareIT, UC Browser, CamScanner and Clubfactory.

The Ministry has banned the apps by invoking Section 69A of the Information Technology Act, 2000 (the IT Act) along with the relevant provisions of the Information Technology (Procedure and Safeguards for Blocking of Access of Information by Public) Rules, 2009 (the Blocking Rules) deeming apps’ *“prejudicial to sovereignty and integrity of India, defence of India, security of state and public order.”* According to the Ministry, the banned apps are accused of *“stealing and surreptitiously transmitting users’ data in an unauthorized manner to servers having locations outside India. The compilation of this data, its mining, analysis and profiling by elements hostile to national security, which ultimately impinges the sovereignty and integrity of India, therefore, is a matter of very deep and immediate concern which requires immediate measures.”*

6.7.1. Violation of Fundamental Rights

The decision to block access to the Chinese apps has significant consequences, as a large number of Indian people use these services regularly. For example, TikTok has more than 100 million active users in India. Along with

¹⁷⁵ Jayant Das, *Increasing intrusion of state into right to privacy* THE PIONEER, Jul 04, 2018, <https://www.dailypioneer.com/2018/state-editions/increasing-intrusion-of-state-into-right-to-privacy.html>

revolutions such as affordable internet, Tik Tok has brought marginalised people online to tell their stories in a way no other app has ever been able to. Transgender, lower caste, villagers, and independent artists from are creating and broadcasting content on TikTok in a way that was previously never thought of and was at the monopoly of only groups with a greater social equity.

Not only is the video app convenient to use, but it is also more accessible as it has given people who don't lead instagrammable lives or even speak English the confidence to showcase their skills and share their lives.

Reports demonstrate how the app gives voice to entrepreneurs and small business owners across rural India. It has also been articulated that the ban has come into being during the pandemic is particularly unfortunate, given the sense of harmony that it provided to these communities.

“Another community that has been severely impacted by the ban on these apps are the Tibetan refugees in Delhi who used We Chat to connect with their families and friends back in Tibet. They also relied on this app to get access to news and other information. They cannot use other widely-used social media applications like Facebook or Whatsapp since they are banned in Tibet. Further, WeChat is easier to use, and voice messaging did not require literacy in Tibetan, enabling refugees who do not read Tibetan to participate.”

“Similarly, in the last 10 years or so, many Indian students have enrolled themselves in Chinese universities. They too were dependent on apps like WeChat to communicate with their colleagues and college administrations.

Any account of freedom of expression that does not consider how this ban will affect marginalised communities is not at all credible. Since apps provide a platform for expression and allow for the dissemination of information are protected by Art.19(1)(a) of the Indian Constitution, a constitutional challenge to the ban is very likely.”

In order for the freedom of speech and expression to be withheld, the right must be inclusive and available to everyone; not just those with the social capital to access applications with relatively complex and difficult user interfaces. This is true because of the extremely low levels of digital literacy in India. The freedom of expression in this context should be understood to include the manner in or the platform on which people wish to express themselves. Further, even if one assumes that the freedom to engage in trade or business is not available to Chinese app makers (presumably non-citizens), they continue to exercise the right against under article 14.

Recently, the Kerala High Court in a case, *“Faheema Shirin v. State of Kerala”*¹⁷⁶ recognizes that, *“interfering with someone’s access to the internet actually violates their fundamental right to privacy.”*

Subsequently, the Supreme Court in *“Anuradha Bhasin v. Union of India”*¹⁷⁷ highlighted that, suspension of the internet could definitely amount to an abuse of power. However, it fell short of affirming the position laid down by the Kerala High Court. However, since the decision in *Faheema Shirin* has not been overruled, it holds persuasive significance and should correctly be assumed to be the correct position of law in this situation. Arguably, there does exist freedom of access to the internet under Article 19, hence, it becomes important to re-evaluate the effect the geoblock on Chinese Apps has on this right.

6.7.2. Whether the application ban is Justifiable

Speaking against the ban, Ji Rong, spokesperson of the Chinese embassy in India, said that the ban violates the World Trade Organization (WTO) rules and “abuses the national security exceptions.” Indian officials are very confident that India can defend the move under this exception. I believe India

¹⁷⁶ 2019(2) KHC 220

¹⁷⁷ WRIT PETITION (CIVIL) NO. 1031 OF 2019.

would be successful in invoking the national security exemption to justify the ban, in the (unlikely) event that China were to approach the WTO.

As a justification, a press release announcing the ban, explained that Indian users' data was being transferred to servers located outside India, in an unauthorised manner. This may lead to the profiling and mining of users' data by elements hostile to the national security and defence of India which was a matter of deep and immediate concern, and required emergency measures.

As we know, the move came after the border clash between Indian and Chinese soldiers in the Galwan Valley, along the Line of Actual Control, resulting in the death of 20 Indian soldiers.

6.7.3. Invoking the National Security Exception under the WTO Framework

The national security exception under the WTO framework has been invoked twice so far –

1. “Russia’s justification of a ban on Ukraine’s trucks from driving within Russia during the Ukraine crisis (Russia/Ukraine decision)” ;
2. “Saudi Arabia’s justification for not initiating criminal procedures against a company which was stealing copyright protected content from a Qatari company (during the blockade against Qatar) (Saudi/Qatar decision).”

While the WTO Panel accepted the justification in case of Russia, it was rejected in the case of Saudi Arabia.

“Article XIV of the General Agreement on Trade in Services (GATS)”¹⁷⁸, “In its operative part, provides that nothing prevents any Member from taking any action which is considered necessary for the protection of its essential security interests” :

¹⁷⁸ Article XIV of the GATS sets out the general exceptions from obligations under that. Agreement in the same manner as does Article XX of the GATT 1994..

- i. relating to the supply of services for the provisioning of a military establishment;
- ii. relating to fissionable and fusionable materials and the materials from which they are derived;
- iii. *taken in time of war or any other international relations emergency.*

India is most likely to take the stand that the ban was necessary for the protection of its essential security interests and that the decision to ban these applications was *taken in the time of war or any other international relations emergency.*

“This phrase also recently came up as an interpretation by the WTO Panel in the Saudi Arabia/Qatar decision. Based on the Panel’s analysis, India *will have to* fulfil three conditions: *first*, there was a situation of ‘war or other emergency in international relations; *second*, such a ban was adopted *during* such war or emergency; and *third* and most importantly, the ban was not remote or unrelated and it was a plausible measure to protect India’s essential security interests.”

6.8. Peroration

At present, there is not sufficient information on precisely how using Chinese apps in India raises national security concerns to such an extent that the general public needs to be completely warranted of these apps. “However, research suggests that Chinese laws require app services to necessarily share user data upon request. Further, a recent study indicated that most Chinese apps (including Helo and Shareit) collect excessive information such as access to microphones, cameras and precise cell-site location information which is not necessary to render services related to the particular application.”

“While this measure objectively indicates that Chinese apps need to increase underlying privacy safeguards, a study comparing the operability of Chinese apps with apps made outside China on play store or apple store is yet to be conducted. In the absence of such a study, a stand-alone review of Chinese

Apps may suffer from the absence of a comparative analysis to fare it in relative terms.” Through a careful comparison by measuring the extent to which Chinese apps relatively raise greater concerns which form the basis of the Notification would help establish the suitability of directing a ban specifically against China. “This would also help corroborate a cogent and rational connection with national security concerns. Singling out all Chinese apps may require some unique basis in order to be considered a ‘suitable’ restriction.”

CONCLUSION

It is quite evident that various governments of the world have been misusing the technological means to invade our privacy in the name of security. Surprisingly, the states which are the champions of peace at the United Nations and members of the Security Council have been the forerunners in the abuse against right to privacy.

Our own country India has followed the steps of its allies and have been vehemently bypassing the right to privacy of the citizens in the name of national security. The last two decades have seen a rise in the incidents since technological advancements have not only made governments more able at doing this, but, also the citizens more prone to snooping. The whole world of the citizens revolve around their smartphones, laptops and other digital devices which make remote snooping not only possible but very easy.

The government's control over telecom and software companies also makes it easier for them to snoop data. Telecom operators share data about our activities on the phone with the government and practically no calls or text we send are private anymore.

Companies like Facebook, Google and whatsapp snoop our data and sell it to the government as well as the highest bidder which makes it more dangerous. Our complete digital profile is up for the government to have, all in the name of national security.

The most dangerous part of data snooping is mass-compulsory data collection programs like the Aadhar. More than a billion people are required to enter into a database, their details as well as their fingerprints. *“Basically a collection of more than a billion lives at the mercy of the government to be*

used as they deem fit. More importantly, guarded by primitive digital security which can be ripped apart by a second grade hacker”¹⁷⁹.

The reality as of today is that the government has authorized its agencies to snoop on its citizens in the name of national security as they feel when it is in clear violation of the *Puttuswamy Judgement*¹⁸⁰ wherein steps were mentioned which have to be met in order to snoop on a citizen.

The data snooping can very well be used by the government to eliminate political competitions by breaching their right to privacy. The power to breach privacy in the name of national security when coupled with the amended law of UAPA arm the government with a dangerous tool which can easily murder democracy.

Any opponent can be snooped thoroughly and titled a terrorist at the whim of the government without a single court order being needed in the entire process. The degree to which this sounds dangerous is unimaginable. This is enough to crush any free speech or remnant of democracy in the country.

The only ray of hope to put a stop to the rampant powers of the government is the Judiciary through its powers to stop the legislature when it oversteps. The usual method being judicial review which has worked in the past very well, however, with the advancement in technology as well as amendments to the UAPA law, the right to privacy is in a much more imminent threat than the past.

There has always been a need for a strong hand to counter terrorism and all such related activities, but if the protection for the citizen came at a cost of gross miscarriage of justice and violating the basic human, if not fundamental rights of an individual, then what good does such a protection

¹⁷⁹ Volume 3 , ROBERT M. CLARK & SIMON HAKIM, CYBER PHYSICAL SECURITY (Springer) ISBN 978-3-319-32822-5

https://www.business-standard.com/article/current-affairs/aadhaar-breach-how-rs-500-is-all-it-takes-to-pry-on-a-billion-indians-118010400169_1.html

¹⁸⁰ Justice K.S. Puttaswamy v. Union of India: (2017) 10 SCC 1

do? The Right to Dissent is one of the core founding principles on which democracies are built, and the UAPA simply tries to take away that right from the people. It is an assault of citizens' right to expression which is also a collective right of groups and unions to disseminate their views and UAPA majorly targets this right. Secondly, it can simply be used to bypass fundamental rights and procedures. For instance, those arrested under UAPA can be incarcerated up to 180 days without a charge sheet being filed. It thus directly violates Article 21 of the constitution. Thirdly, it confers upon the government broad discretionary powers and also authorizes the creation of "special courts with the ability to use secret witnesses and to hold closed-door hearings."¹⁸¹

Several provisions of the Unlawful Activities (Prevention) Act, 1967, were authoritative, as well as overly broad in their definition, thereby allowing the government to do a large number of things over a simple authority, just because it wasn't specific enough to point out as to what it was actually referring to.¹⁸²

The Jammu and Kashmir Police arrested the Journalist Masrat Zahra under Section 13 of the Unlawful Activities (Prevention) Act, 2020 by stating that she uploaded anti-national videos on Facebook to incite the youth in glorifying anti-national activities. They also put this same draconian provision on Peerzada Ashiq when she posted about the diversion of COVID testing kits, stating that, it is against the authorities. The Amnesty International Executive Director called such acts by the Indian Government as an attempt to curb the right to freedom of expression of its citizens.¹⁸³

The Jammu and Kashmir police had also invoked Section 13 of UAPA against people who were accessing social media through VPN's to dodge

¹⁸¹ Chapter VII of the Unlawful Activities (Prevention) Act, 1967, As amended by the 2010 amendment.

¹⁸² Unlawful Activities (Prevention) Act, 1967, Sec 3, Sec 2 .

¹⁸³ *J&K Police Using Repressive Counter Terrorism Law To Muzzle Access To Social Media*, AMNESTY INTERNATIONAL INDIA.

<https://amnesty.org.in/news-update/jk-police-using-repressive-counter-terrorism-law-to-muzzle-access-to-social-media/> (Last Visited: Aug 1, 2020)

the longest ever internet ban imposed by the government when it scrapped Article 370 of the constitution to divide the state into two centrally administered UT's. The government said that it was done "to curb the misuse of the sites by miscreants for propagating false information/rumors."¹⁸⁴

Desperate times indeed call for desperate measures, and history is a brave example that no matter how desperate one gets, nothing is above the human rights of an individual. The way the UAPA has been drafted clearly puts it in par with the USA PATRIOT Act, which was criticized way too much for being violative of fundamental rights.¹⁸⁵ In essence, from a neutral standpoint, there is no way an act like the UAPA should exist in a democracy like India, unless we are already an "Orwellian State"¹⁸⁶ like the U.S.

Data snooping is something which has always been looked down upon since time immemorial. Upon looking at incidents around the globe, one would easily identify one of the biggest incidents of data snooping which was Edward Snowden blowing the whistle on the NSA.¹⁸⁷ The United States came under heavy criticism globally¹⁸⁸ after the world came to understand the extent to which the NSA was surveilling i.e. not only limited to the

¹⁸⁴ *Panic in Kashmir as case filed against social media users*, AL-JAZEERA, Feb. 8, 2020

<https://www.aljazeera.com/news/2020/02/panic-kashmir-cases-filed-social-media-users-200218114417864.html>
(Last Visited: 01st August, 2020)

¹⁸⁵ Dustin Volz, *Opposing Trump, conservative bloc demands reforms to internet spy law*, REUTERS, Jun.16, 2017

<https://www.reuters.com/article/us-usa-intelligence/opposing-trump-conservative-bloc-demands-reforms-to-internet-spy-law-idUSKBN1962SR> (Last Visited: 01st August, 2020)

¹⁸⁶ "Orwellian" is an adjective describing a situation, idea, or societal condition that George Orwell identified as being destructive to the welfare of a free and open society. It is used to describe a political system in which the government tries to control every part of people's lives, similar to that described in the novel "Nineteen Eighty Four", by George Orwell.

¹⁸⁷ *Edward Snowden: Leaks that exposed US spy programme*, BBC NEWS, Jan. 17 2014.

¹⁸⁸ *Malaysia protests at 'US and Australia spying' in Asia*, BBC NEWS, Nov. 2, 2013 .

<https://www.bbc.com/news/world-asia-24784895>;

citizens of the US, but also citizens of other countries, including India.¹⁸⁹ Therefore, for India to be walking on the exact same steps as a nation who has been continuously accused for gross violations of human rights is a sign of authoritarianism. Being snooped in the democracy, which would further change the status quo of how things are handled within the nation. Hence, something as deplorable as what the US did shouldn't be done by India yet again.

The speed at which a person's privacy can be abused and his rights usurped is dangerously high and therefore the judiciary has to be far more active than just judicial review.

Looking at the mammoth amounts of evidence present in front of us when it comes to violation of right to privacy, and the outburst to when it is violated, it is clearly not in the favour of our government, or the nation, to make a mockery out of the nation by going in for an unplanned idea which is responsible for keeping the personal data of millions of Indians, including biometrics. Further, what's worse is the fact that when the government is actually criticized on how they are handling the data of millions of their citizens, instead of appreciating the gesture and making the necessary changes to make the system a more secured one, the government went on to harass and prosecute those who actually revealed the said informatio.¹⁹⁰ Punishing the person who reveals your mistake is not only a coward's move, it shows the extent to which the government will go to silence a person who speaks against the plans of the government. This shows that the democracy is slowly moving towards autocracy and dictatorship, and when a government starts doing such horrors while in power, it is always the duty of the judiciary to put things in check. The Supreme Court of India might've held mandating the aadhar in certain things as a violation of fundamental

¹⁸⁹Glenn Greenwald, Shobhan Saxena, *India among top targets of spying by NSA*, THE HINDU, Sep. 23, 2013 <https://www.thehindu.com/news/national/india-among-top-targets-of-spying-by-nsa/article5157526.ece>

¹⁹⁰Rahul Bhatia, *Critics of Aadhaar project say they have been harassed, put under surveillance*, REUTERS, Feb. 13, 2018 / 11:11 AM <https://www.reuters.com/article/india-aadhaar-breach/critics-of-aadhaar-project-say-they-have-been-harassed-put-under-surveillance-idINKBN1FX0FU>

rights¹⁹¹, but it is just a tip of the iceberg and there is a pretty long way to go before all the wrongs of the government could be rectified.

It has to do judicial activism to nip the threats in the bud.

In the ever-increasing invasion of the state into the right to privacy, it has become necessary for the entire community to have seminars on the concept growth and implementation of the concept and the law relating to Right to Privacy.

Just as national security is paramount to the state; in the same manner right to privacy is paramount to personal liberty of the individuals. The problem thus is to harmonize these two conflicting interest. While in the interest of national security it might be inevitable for the state to adopt measures which may have the undesirable effect of interfering of the privacy of an individual, it is necessary to ensure that the state does not assume to itself an unbridled and unfettered power to encroach upon the privacy of the individuals in the name of national security. Certain measure and guidelines must be formulated within the prescribed limits of which only the state can interfere with the privacy of the individual. In this regard a visit to the judgment and the view held in *KS Puttuswamy*¹⁹² would be appropriate and it must be followed in the letter as well as in the spirit.

A Public Interest Litigation has been filed by one Sajal Awasthi¹⁹³ asking the Supreme Court to declare the UAPA as unconstitutional because it is violative of the Fundamental Rights of the citizens. He goes on to explain that the right to dissent is one the very basic rights of an individual and the curtailing the same would be grossly against Articles 14,19, and 21 of the Constitution of India. He also states that the act does not provide any

¹⁹¹ *Aadhaar not mandatory for bank account, mobile number but must for ITR*, LIVE MINT, 27 Sep 2018, <https://www.livemint.com/Politics/wBZFzYhxzw8p2MO3rk5UyI/aadhaar-UGC-neet-CBSE-exams-bank-account-PAN-mobile-ITR.html>

¹⁹² *Supra* at 173.

¹⁹³ SUPREME COURT OF INDIA, CIVIL ORIGINAL JURISDICTION WRIT PETITION (CIVIL) NO. 2019

opportunity to the person arrested to prove that he is not a terrorist, which is very arbitrary to the core. He further went on to say that:-

“Right to Reputation is an intrinsic part of [a] fundamental right to life with dignity under Article 21 of the Constitution of India and terming/tagging an individual as ‘terrorist’ even before the commencement of trial or any application of judicial mind over it, does not adhere to procedure established by law.”

The Association for Protection of Civil Rights (APCR) filed another petition in the Supreme Court challenging Section 35 of the UAPA, because after the 2019 amendment it allows the Government to label an individual as a terrorist, whilst before the same could only be done to organizations and associations.

While PILs such as these definitely go a long way in paving a path for the protection of individual freedom and fundamental rights, they definitely aren't enough to ensure that each and everything which the government does is kept in check. Further, PILs most certainly cannot be our only line of defense against government autocracy, for if the people have to come down and defend themselves at every instance of wrongdoing then we might as well start living in an anarchist state, because the Judiciary is as good as sitting ducks if it doesn't act until poked when a wrong is done. Judicial activism is not only important, it is necessary at the moment to insure that the rights and freedoms of an individual aren't stepped upon every now and then when the government feels it has the right to do so. The government is elected by the people, therefore it must always have a sense of responsibility towards the people itself and not work recklessly to hamper the rights of the individuals it is so responsible to protect.

After understanding the intricacies, according to me, the first and the foremost step should be to establish a synergy between both the necessary evils; the right to privacy is a basic fundamental right but national security is no joke! For this stint to successfully and legally operate without violation of the data security laws and without infringement of the privacy laws, it is

very important that there should be inclusion of judiciary in national security.

One Apex committee should be formed with the members from Supreme Court to keep checking the involvement of legislature into the functions of national security branches like CBI and IB.

A mandatory court order to launch full-fledged snooping operation on an individual under peace-time mission should be protocol to ensure rule of law as well as protect immediate actions for security from these processes.

Third and the most important thing that can be done is, to put in a heavy investment to build strong cyber protection wing so that the data of the citizen collected for sovereign use may not fall in the hands of hostile powers.

Acts such as the UAPA and the NIA need to have strict provisions with regard to bail and remand so that the investigation agencies do not abuse the powers regarding arrest and unlawful detention. Agencies have been accused numerous times of using the UAPA to harass critics and detain them for unreasonably long periods.¹⁹⁴ Records also further show that almost 2/3rd of the cases filed under UAPA get dismissed soon after being filed. Hence it shows a sleazy attempt by the authorities to use it as a disguise to harass individuals.¹⁹⁵

To put the final nail to the coffin, the Government actually went forward and included Section 18¹⁹⁶ of the Unlawful Activities (Prevention) Act, 1967, which stated that No Legal Proceeding shall lie against the government for any loss or damage caused because of any action taken by

¹⁹⁴ *UAPA Being Misused to Confine Political Prisoners Endlessly: PUDR*, THE QUINT, 01 Oct 2018.

<https://www.thequint.com/news/india/activist-arrest-bhima-koregaon-how-uapa-being-misused-pudr>

¹⁹⁵ Chaitanya Mallapur & Devyani Chhetri, *Arrested activists: 67% ended in acquittal or discharge under UAPA Act*, BUSINESS STANDARD, Sept. 14, 2018

https://www.business-standard.com/article/current-affairs/arrested-activists-67-ended-in-acquittal-or-discharge-under-uapa-act-118090800801_1.html

¹⁹⁶ Section 49 of the Present UAPA Act.

the Government while acting under the powers of the said act. This actually gave the government full immunity from any kind of responsibility which may arise from the continuous use of the said act. No one should be free from any kind of accountability, the least of those being the government who is actually using such unfettered powers to harass individuals. Provisions like this which give the government a license to openly go ahead and abuse their powers should be the first ones to be actually struck down.

Next, the government needs to stop harassing the whistleblowers, or start going after them solely because they chose to list out the flaws in the program which the government was already running or planning on running. The government doing such acts clearly suggests that the government simply raises an issue with the free speech in the nation, and therefore free speech is questionable.

Furthermore, As suggested by a number of learned scholars and activists and rational thinkers, UIDAI should focus on the localization of data in India. With a number of firms hosting data outside of India, it is only so long before there is a malware attack or some kind of hack which once again puts the data of millions of people at risk. Rajya Sabha MP Subramaniam Swamy even went on to say that in California, any software specialist can download for aadhar data for as little as \$50.¹⁹⁷

As known by us and the masses, There's an attack on the government websites time and again and it is served by hackers outside of the borders, as well as breach of Aadhar database raises an eyebrow on the government collecting data from its citizens and failing miserably at protecting it.

In addition to the aforementioned list of things, There needs to be a greater transparency in the system than there is in the current system. Government agencies are not accountable to anyone other than the government itself. A comprehensive reform of the surveillance framework in India is long overdue.

¹⁹⁷ Rachel Chitra , *UIDAI to look seriously into data localisation compliance*, ET PRIME, April 16, 2019.

The current debate, therefore, is not about ‘whether surveillance at all’, but about ‘how, when, and what kind of surveillance’.

This is also the right time: Across the world, there is an increasingly urgent debate about how to protect basic rights against encroachment by an aggressive and intrusive state, which wields the rhetoric of national security like a sword.

In India, the Supreme Court’s privacy judgment has taken a firm stand on the side of rights. Citizens’ initiatives, such as the Indian Privacy Code have also proposed legislative models for surveillance reform.

After the Supreme Court’s 2017 judgment in *K.S. Puttaswamy v. Union of India* (‘the Right to Privacy case’), the Constitutional contours within which the questions of ‘how, when, and what kind’ have to be answered have been made clear.

Any impingement upon the right to privacy must also be proportionate

One of the factors of the proportionality standard is that the government’s action must be the least restrictive method by which a state goal is to be realized. In other words, if the same goal — i.e., protecting national security can be achieved by a smaller infringement upon fundamental rights, then the government is Constitutionally bound to adopt the method that does, indeed, involve minimal infringement.

Reforms in the Indian surveillance regime, should, therefore, incorporate ethics of surveillance which considers the moral aspects of how surveillance is employed.

Lastly, *“The regime is opaque. There is almost no information available about the bases on which surveillance decisions are taken, and how the legal standards are applied. Indeed, the evidence seems to suggest that there are none: a 2014 RTI request revealed that, on an average, 250 surveillance requests are approved every day. It stands to reason that in a situation like*

this, approval resembles a rubber stamp more than an independent application of mind.”¹⁹⁸

Even though the staunchest civil rights advocates will not deny that an individual reasonably suspected of planning a terrorist attack should be placed under surveillance, in this context, the evidence demonstrates clearly that a heavily bureaucratized and minimally accountable regime of surveillance does nothing to enhance security, but does have significant privacy costs.

“For example, while examining the U.S. National Security Agency’s programme of mass surveillance, an American court found that out of more than 50 instances where terrorist attacks had been prevented, not even a single successful pre-emption was based on material collected from the NSA’s surveillance regime.”

In India, the existing surveillance framework is complex and confusing. Simply put, two statutes control the field: telephone surveillance is sanctioned under the 1885 Telegraph Act (and its rules), while electronic surveillance is authorized under the 2000 Information Technology Act (and its rules).

*“This framework is heavily bureaucratized. “Decisions about surveillance are taken by the executive branch (including the review process)”*¹⁹⁹ with no parliamentary or judicial supervision; indeed, the fact that an individual will almost never know that she is under surveillance, means that finding out about surveillance, and then challenging it before a court, is a near-impossibility.”

*“The surveillance regime is also vague and ambiguous. Under Section 69 of the IT Act, the grounds of surveillance have been simply lifted from Article 19(2) of the Constitution, and pasted into the law.”*²⁰⁰ They include very wide phrases such as “friendly relations with foreign States” or “sovereignty and the regime is justified as it strikes a pragmatic balance between the competing values of privacy and security.

¹⁹⁸ Gautam Bhatia, *The case against surveillance*, THE HINDU, December 25, 2018 .

¹⁹⁹ Paz Peña O , *The bureaucratization of surveillance*, THE MEDIUM, August 31,2017.

<https://medium.com/@pazpena/the-bureaucratization-of-surveillance-682c7d27401f>

²⁰⁰ *Id* at 192

European Union general data protection regime on non-personal data :

“In May 2019, the EU came out with a regulatory framework for the free flow of non-personal data. It suggested that member states of the union would cooperate with each other when it came to data sharing. Such data, the EU had then ruled would be shared by member states without any hindrances.”²⁰¹

*“The authorities must inform the commission of any draft act which introduces a new data localisation requirement or makes changes to an existing data localisation requirement.”*²⁰²

“What areas does India’s non-personal data draft miss? Though the non-personal data draft is a pioneer in identifying the power, role, and usage of anonymised data, there are certain aspects such as community non-personal data, where the draft could have been clearer. Non-personal data often constitute protected trade secrets and often raises significant privacy concerns. The paper proposes the nebulous concept of community data while failing to adequately provide for community rights.”

“Other experts also believe that the final draft of the non-personal data governance framework must clearly define the roles for all participants, such as the data principal, the data custodian, and data trustees.”

When considering “The Unlawful Activities (Prevention) Amendment Act, 2019, it seeks to substantially modify Chapter VI of the Unlawful Activities (Prevention) Act, 1967 and Section 35 and 36 therein. The new Section 35 of the UAPA Act, 1967 empowers the Central government to categorise any individual as ‘terrorist’ and add name of such a person in Schedule 4 of the Act,”²⁰³ But the, “Right to reputation was an intrinsic part of fundamental right to life with dignity under Article 21 of the Constitution and tagging an individual as “terrorist” even before the commencement of trial or any application of judicial mind over it, did not amount to following the procedure established by law.”

²⁰¹ Aashish Aryan, *Explained: What is non-personal data?* , THE INDIAN EXPRESS , July 27, 2020 <https://indianexpress.com/article/explained/non-personal-data-explained-6506613/>

²⁰² *Id.*

²⁰³ *UAPA amendment: respond to pleas, apex court tells govt* , THE HINDU, Sep. 6, 2019

The right of dissent is a part and parcel of fundamental right to free speech and expression and therefore, cannot be abridged in any circumstances except for mentioned in Article 19 (2). The UAPA, 2019 empowers the ruling government, under the garb of curbing terrorism, to impose indirect restriction on right of dissent which is detrimental for our developing democratic society

There is a need to strike a fine balance between privacy and ensuring that policing or national security is taken to a level where technology is a facilitator and not a hindrance for integrity of India

BIBLIOGRAPHY

STATUTES

1. Constitution of India, 1950
2. Information Technology Act, 2000
3. Indian Penal Code, 1860
4. Credit Information Companies Regulation Act, 2005
5. The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

BOOKS

1. Basu, Durga Das: Commentary on Constitution of India, Lexis Nexis, 8th edn., vol. 6, 2010.
2. Jain, M.P.: Constitutional Law: Fundamental Right, Lexis Nexis, 7th edn., 2014.
3. Ravinder Kumar and Gaurav Goyal: The Right to Privacy in India: Concept and Evolution, Partridge India Publication, 2016.
4. S.K. Sharma, Privacy Law: A Comparative Study, Atlantic Publishers & Dist. Publication, 1994.
5. Marta Otto: The Right to Privacy in Employment: A Comparative Study, Bloomsbury Publishing, 2016.
6. Richard A. Glenn: The Right to Privacy: Rights and Liberties Under the Law, ABC-CLIO Publication, 2003.
7. Adam Carlyle Breckenridge: The Right to Privacy, U of Nebraska Press, 1970.
8. Brandon Garrett: The Right to Privacy, Individual freedom, civic responsibility, The Rosen Publishing Group, 2001.
9. David L. Hudson: The Right to Privacy, Infobase Publishing, 2009.

10. Caroline Kennedy and Ellen Alderman: *The Right to Privacy*, Knopf Doubleday Publishing Group, 2010.

JOURNALS AND ARTICLES

1. Vrinda Bhandari and Renuka Sane: “Towards a privacy framework for India in the age of the Internet”, (November 2016), Working Paper No. 179, NIPFP Working Paper Series.

2. Namit Oberoi: “The Right to Privacy: Tracing the Judicial Approach Following the Kharak Singh Case”, *INJConLaw* 11; (2007) 1 *Indian Journal of Constitutional Law* 216.

3. Gautam Bhatia: “State Surveillance and The Right to Privacy in India: A Constitutional Biography”, (2014) 26(2) *National Law School of India Review* 127.

4. Anubhav Khamroi and Anujay Shrivastava: “The Curious Case of Right to Privacy in India”, *Indian Constitutional Law Review, Quarterly Law Journal* (2017).

5. Aashit Shah and Nilesh Zacharias: “Right to Privacy and Data Protection”.

6. Daniel J. Solove: “Conceptualizing Privacy”, 90 *Calif. L. Revs.* 1087 (2002).

7. Adam D. Moore: “Privacy: Its Meaning and Value”, Vol. 40, No. 3, Jul., 2003.

8. Neeraj Grover: “Right to Privacy in Digital Age: Evolving Privacy Laws and Their Applicability to Social Media” (2011).

9. Afshan Nazir and Ayush Gupta: “Right to Privacy: Fundamentally Ours” (2017).

10. Suhrith Parthasarathy, “Privacy, Aadhar and the Constitution” (2017). *Indian National Security and Counter-Insurgency: The Use of Force Vs Non-violent Response*; ISBN 978-1-134-51431-1

11. Black Friday – The True Story of the Bombay Bomb Blasts; ISBN 978-0-14-302821-5
12. Nitya Ramakrishnan, Tortured, Humiliated, But Unbroken: An Interview With S.A.R. Geelani, *The Wire*, Oct. 25, 2019.
13. Special Correspondent, Police bid to intimidate Kawalpreet, claims AISA, *THE HINDU* (Apr. 29, 2020).
14. Ujjaini Chatterji, UN Special Rapporteurs express concerns over UAPA, *THE LEAFLET* (May 18, 2020).
15. Aakar Patel, UAPA (Amendment) Bill 2019 violates the very international laws it quotes, defies principles of natural justice, *Firstpost*, (Aug. 3, 2019)
16. UAPA amendment: respond to pleas, apex court tells govt , *The Hindu*, Sep. 6, 2019
17. Paz Peña O , The bureaucratization of surveillance, *The Medium*, August 31,2017.
18. Gautam Bhatia, The case against surveillance , *The Hindu*, December 25, 2018 .
19. Aashish Aryan, Explained: What is non-personal data? , *The Indian Express* , July 27, 2020
20. Daniel J. Solove, Conceptualizing Privacy, *California Law Review*, Vol. 90, No. 4 (2002),
21. Alessandro Acquisti, Privacy in Electronic Commerce and the Economics of Immediate Gratification H. John Heinz III School of Public Policy and Management, Carnegie Mellon University
22. Aarushu sahu ,Evolution of Right to privacy,legal bites ,Jan 15 2018
23. William M. Beaney, “The Right to Privacy and American Law”, *DUKE L.J.* (1965)

24. Ananya Chakraborty, “The U.S. Should Adopt the 'Right to Be Forgotten”, NEWS 18 INDIA, Aug 24, 2017
25. Vinita Bali , Data Piracy: Can India Provide Adequate Protection for Electronically Transferred Data? Clara Law Digital Commons, 21 Temp. Int'l & Comp. L. J. 103 (2007)
26. Maj Gen Sheru Thapliyal, 1962 War: A Critical Analysis, Mar. 30, 2018,
27. Namrata Goswami, Indian National Security and Counter-Insurgency: The Use of Force Vs Non-violent Response, ROUTLEDGE,43. ISBN 978-1-134-51431-1
28. Vishwa Mohan & Anam Ajmal, “Cops use UAPA to block site, call it ‘goof-up’ later”, The Times of India, Jul 24, 2020
29. J&K Police Using Repressive Counter Terrorism Law To Muzzle Access To Social Media”, Amnesty International India, Feb 18, 2020.
30. Deepali Bhandari & Deeksha Pokhriyal, The Continuing Threat of India’s Unlawful Activities Prevention Act to Free Speech, JURIST, Jun 2, 2020.
31. Editorial, “Panic in Kashmir as case filed against social media users”, Al-Jazeera, Feb 18,2020.
32. Deepali Bhandari & Deeksha Pokhriyal, The Continuing Threat of India’s Unlawful Activities Prevention Act to Free Speech, JURIST, Jun 2, 2020.
33. Editorial, “Panic in Kashmir as case filed against social media users”, Al-Jazeera, Feb 18,2020.
34. Dustin Volz, “Opposing Trump, conservative bloc demands reforms to internet spy law” , REUTERS, Jun. 16, 2017.
35. Abdul Wahid Shaikh, Interview: Of Torture, Impunity and the False Charges on Abdul Wahid Shaikh ,THE WIRE, May 20, 2017.
36. When Poetry is held Unlawful: A Case of Kabir Kala Manch, INDIA RESISTS, Apr. 23, 2015

37. Devika Kohli, “Why Is The Government So Threatened By A Man Who Is 90% Disabled?”, YKA, May 19, 2015.
38. AISA’s Delhi head booked under UAPA by Crime Branch, mobile seized, INDIAN EXPRESS, Apr. 29, 2020.
39. First Post Staff, Masrat Zahra booked under UAPA: Kashmiri photojournalist's work focussed mostly on women, conflict reporting in Valley, FIRSTPOST, Apr. 20, 2020.
40. Kiran Rathee, “Govt plans to link driving licence with Aadhaar,” Business Standard, Sep 26,2018.
41. Editorial, “Supreme Court counters push for Aadhaar,” The Hindu, Mar 27, 2017.
42. IANS, “Rajya Sabha returns Aadhaar bill to Lok Sabha with amendments,” Hindustan Times, Mar 16,2016.
43. Editorial, “Aadhaar bill is through after Opposition scores a few brownie points,” Indian Express, Mar 17, 2019.<http://indianexpress.com/article/india/india-news-india/rajya-sabha-returns-Aadhaar-bill-to-lok-sabha-with-oppn-amendments>.

April 23, 2015

ONLINE WEBSITES

1. <http://plato.stanford.edu/entries/privacy>
2. <http://www.jstor.org/stable/3481326?origin=JSTOR-pdf>
3. <http://ssrn.com/abstract=2040940>
4. <https://www.legalbites.in/evolution-right-privacy-india>
5. <http://www.rtifoundationofindia.com/evolution-right-privacy-india#.WvabwIiFM2w>
6. <http://thelegiteye.in/2017/10/24/case-analysis-right-privacy>

7. <http://gilc.org/privacy/survey/intro.html>
8. https://lawreview.law.ucdavis.edu/issues/43/3/liberty/43-3_Greene.pdf
9. <https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=3107&context=lcp>
10. www.intelligencesquaredus.org .
11. <https://www.news18.com/news/india/right-to-privacy-verdict-how-other-countries-have-dealt-with-the-issue-1499985.html>
12. <http://indianexpress.com/article/india/right-to-privacy-how-it-is-protected-in-other-countries/>
13. http://www.business-standard.com/article/economy-policy/govt-plans-to-link-driving-licence-with-aadhaar-117091600042_1.html
14. <http://www.thehindu.com/news/national/aadhaar-cannot-be-mandatory-for-welfare-schemes-supreme-court/article17671381.ece>.
15. <http://www.hindustantimes.com/india/rajya-sabha-returns-aadhaar-bill-to-lok-sabha-with-amendments/story-uCVCaTLOVVyOVwrHqEuOSI.html>
16. <http://indianexpress.com/article/india/india-news-india/rajya-sabha-returns-Aadhaar-bill-to-lok-sabha-with-oppn-amendments>
17. <https://thewire.in/145800/sc-upholds-law-link-aadhaar-pan-grants-partial-stay/>
18. http://www.business-standard.com/article/companies/reliance-jio-does-a-u-turn-admits-to-data-leak-in-police-complaint-117071300193_1.html
19. <http://indianexpress.com/article/india/supreme-court-to-review-section-377-homosexuality-gay-lesbians-all-your-questions-answered-5016319/>
20. <http://www.newindianexpress.com/nation/2018/jan/09/relook-at-section-377-comes-after-right-to-privacy-held-as-fundamental-right-1748409.html>

21. <https://www.firstpost.com/india/section-377-what-two-recent-sc-judgments-tell-us-about-courts-altered-view-on-sexuality-and-privacy-in-india-4295821.html>
22. <http://www.bgr.in/features/privacy-why-it-is-important-for-users-to-protect-their-own-data/>
23. <https://www.indiatoday.in/india/story/right-to-privacy-fundamental-right-parliament-1031136-2017-08-24>
24. <http://www.iclg.co.uk/practice-areas/data-protection/data-protection2016/india>
25. <https://byjus.com/free-ias-prep/data-privacy-and-protection-bill-2017>
26. <http://www.thedialogue.co/analysis-draft-data-privacy-protection-bill-2017/>
27. <http://www.legaleraonline.com/articles/data-privacy-and-protection-bill-2017-what-to-expect>
28. <https://www.pillsburylaw.com/en/news-and-insights/data-protection-laws-in-india.html>
29. Office of the Commissioner of Human Rights: www.ochcr.org
30. Amnesty International India: www.amnesty.org.in
31. Al-Jazeera: www.aljazeera.com
32. Reuters: www.reuters.com
33. LiveLaw: www.livelaw.in
34. SC Observer: www.scobserver.com
35. SATP: www.satp.org
36. Indian Defence Review: www.indiandefencereview.com
37. The Wire: www.thewire.in

- 38 The Times of India: www.timesofindia.indiatimes.com
- 39 <https://www.intelligence.senate.gov/sites/default/files/documents/CRPT-113srpt288.pdf>
- 40 <https://thewire.in/rights/sar-geelani-custodial-torture-nitya-ramakrishnan> (Last Visited: 01st August, 2020).
- 41 <https://www.thehindu.com/news/cities/Delhi/police-bid-to-intimidate-kawalpreet-claims-aisa/article31462959.ece>
- 42 <http://www.hindustantimes.com/india/rajya-sabha-returns-aadhaar-bill-to-lok-sabha-with-amendments/story->
- 43 <http://www.thehindu.com/news/national/aadhaar-cannot-be-mandatory-for-welfare-schemes-supreme-court/article17671381.ece>.
- 44 http://www.business-standard.com/article/economy-policy/govt-plans-to-link-driving-licence-with-aadhaar-117091600042_1.html.(visited on March 3, 2018).
- 45 <https://www.firstpost.com/india/masrat-zahra-booked-under-uapa-kashmiri-photojournalists-work-focussed-mostly-on-women-conflict-reporting-in-valley-8278721.html>
- 46 <https://www.newindianexpress.com/cities/delhi/2020/apr/29/aisas-delhi-head-booked-under-uapa-by-crime-branch-mobile-seized-2136830.html>
- 47 <https://www.youthkiawaaz.com/2015/05/gn-saibaba-arrest/>
- 48 <https://indiaresists.com/when-poetry-is-held-unlawful-a-case-of-kabir-kalamanch/>
- 49 <https://thewire.in/law/abdul-wahid-shaikh-acquitted-interview>
- 50 <https://theleaflet.in/un-special-rapporteurs-express-concerns-over-uapa/>
- 51 <https://medium.com/@pazpena/the-bureaucratization-of-surveillance-682c7d27401f>

52. <https://medium.com/@pazpena/the-bureaucratization-of-surveillance-682c7d27401f>
53. <https://thewire.in/law/abdul-wahid-shaikh-acquitted-interview>
54. <https://www.aljazeera.com/news/2020/02/panic-kashmir-cases-filed-social-media-users-200218114417864.html>
55. <https://www.aljazeera.com/news/2020/02/panic-kashmir-cases-filed-social-media-users-200218114417864.html>
56. <https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=3107&context=lcp>. (visited on April
57. Available at: <http://www.jstor.org/stable/3481326?origin=JSTOR-pdf>. (visited on Feb 20, 2018).
58. <https://www.jurist.org/commentary/2020/06/bhandari-pokhriyal-uapa-free-speech/>
59. <https://www.aljazeera.com/news/2020/02/panic-kashmir-cases-filed-social-media-users-200218114417864.html>
60. <http://www.indiandefencereview.com/spotlights/1962-war-a-critical-analysis/> (Last Visited: 01st August, 2020)