RIGHT TO PRIVACY VIS-À-VIS DATA PROTECTION WITH SPECIAL REFERENCE TO THE AADHAAR (TARGETED DELIVERY OF FINANCIAL AND OTHER SUBSIDIES, BENEFITS AND SERVICES) ACT, 2016

Dissertation submitted to the Central University of Punjab

For the award of

Master of Laws

In

Department of Law

By

Nitin Shukla

Supervisor

Dr. Puneet Pathak

Department of Law
School of Legal Studies and Governance
Central University of Punjab, Bathinda
May 2018

DECLARATION

I declare that the dissertation entitled “RIGHT TO PRIVACY VIS-À-VIS DATA PROTECTION WITH SPECIAL REFERENCE TO THE AADHAAR (TARGETED DELIVERY OF FINANCIAL AND OTHER SUBSIDIES, BENEFITS AND SERVICES) ACT, 2016” has been prepared by me under the guidance of Dr. Puneet Pathak, Assistant Professor, Department of Law, School of Legal Studies and Governance, Central University of Punjab, Bathinda. No part of this dissertation has formed the basis for the award of any degree or fellowship previously.

Nitin Shukla
Department of Law
School of Legal Studies and Governance
Central University of Punjab
Bathinda - 151001
Date:

CERTIFICATE

I certify that Nitin Shukla has prepared his dissertation entitled "RIGHT TO PRIVACY VIS-À-VIS DATA PROTECTION WITH SPECIAL REFERENCE TO THE AADHAAR (TARGETED DELIVERY OF FINANCIAL AND OTHER SUBSIDIES, BENEFITS AND SERVICES) ACT, 2016" for the award of LL.M. Degree of the Central University of Punjab, under my guidance. He has carried out this work at the Department of Law, School of Legal Studies and Governance, Central University of Punjab, Bathinda.

Dr. Puneet Pathak
Assistant Professor
Department of Law
School of Legal Studies and Governance
Central University of Punjab
Bathinda - 151001
Date:

ABSTRACT

RIGHT TO PRIVACY VIS-À-VIS DATA PROTECTION WITH SPECIAL REFERENCE TO THE AADHAAR (TARGETED DELIVERY OF FINANCIAL AND OTHER SUBSIDIES, BENEFITS AND SERVICES) ACT, 2016

Name of Student	:	Nitin Shukla
Registration Number	:	16llmlaw03
Degree for which submitted	:	Master of Laws
Name of Supervisor	:	Dr. Puneet Pathak
Name of Centre	:	Department of Law
Name of School	:	School of Legal Studies and Governance
Key words	:	Privacy, Data Protection, Aadhaar, Biometric, Constitution

Privacy is one of the important rights naturally inherited by human being, it has many facets which depend upon the society and person's personal limitation, as the right privacy is recognized under the various international and regional human rights instruments as well as in the constitution of various states. Now, privacy in India stands as the fundamental right under the right to life and personal liberty Article 21 of the constitution of India. Rapid technological advancement in 21st century led to drastic change in the life style of individual. In the era of Information technology, where life is much dependable on technology and various biometric and demographic information is available in the form of data, the issue of privacy of such information is crucial due to the vulnerability of such information. However the gravity of privacy depends upon the data transmitted and the nature of metadata. Under various programme of digital India, Aadhaar project is one of the leading projects to develop the secure and fair system of identity by Government of India for delivery of various services, benefits and subsidies to its citizens. The data collected under the Aadhaar project includes biometric and demographic information of citizen. Such data is sensitive in nature and need exhaustive policy

and mechanism in order to avoid its misuse. Analytical and descriptive method of research are applied during the research. Privacy is the intrinsic part of liberty and human dignity. Though privacy is vital in one's life but it should be balanced with the larger interest. Although Aadhaar Act, 2016 aimed at the delivery of essential services to targeted beneficiary adequately, But the Act has certain loopholes in reference to data protection. Urgent need to revisit the Act in present scenario.

Nitin Shukla Dr. Puneet Pathak

Dedication

I would like to dedicate my current research study in the loving memories of my father late Mr. Siddh Kumar Shukla. He was the epitome of knowledge and positivity who constantly encouraged me. I am thankful to him in numerous ways.

Nitin Shukla

ACKNOWLEDGEMENT

It’s a great pleasure for me to acknowledge the kind of help and guidance received by me during my research work. I sincerely thank my supervisor Dr. Puneet Pathak, Assistant Professor, Department of Law, Central University of Punjab, an amiable personality, for assigning such a challenging research work which has enriched my work experience. I am grateful for his extended guidance, encouragement, support and timely reviews.

I would like to give my special thanks to Prof. P. Ramarao, Dean Academic Affairs without their constant help, support and encouragement, this dissertation would not have been possible. I would also like to thanks, Dr. Tarun Arora HOD, Dr. Deepak Chauhan, Dr. Sukhwinder Kaur, Dr. Amit Kashyap, Department of Law for their valuable suggestions and immense knowledge which they reciprocated throughout.

I owe a special thanks and grateful regards to my friend Ms. Samia Rizvi for extending her enormous help, affection and moral support. Secondly, I would like to express my gratitude to my friends Satish, Vriti, Vikrant, Sukhi, Jameel, Divanshu, Rupal and Aishwarya for always supporting and believing in me with such huge friendliness. My thanks extend to the staff of Computer lab and University library, Central University of Punjab, for providing me all kind of academic and technical assistance during the research work.

Lastly, I am eternally grateful to my family for their support along the course of this research work by giving encouragement and providing the moral and emotional support.

Nitin Shukla

TABLE OF CONTENTS

Table of Cases

LIST OF APPENDICES

LIST OF ABBREVIATION

S. No.	Full form	Abbreviation
1.	All India Reporter	AIR
2.	Central Identities Data Repository	CIDR
3.	Constituent Assembly	CA
4.	European Court	EU
5.	Fleet street Reports (UK)	FSR
6.	Harvard Law Review	HRL
7.	Identification	ID
8.	Information and Communication Technology	ICT
9.	Information Technology	IT
10.	Queen's Bench	QB
11.	Supreme Court Cases	SCC
12.	Supreme Court Reporter	SCR
13.	Unique Identification Authority Of India	UIDAI
14.	United Kingdom	UK
15.	United States	US
16.	United States America	USA
17.	Universal Declaration of Human Right	UDHR

Chapter 1

Introduction

Framework of the Study

Background of study

According to world, Stats Report (2017) nearly 51.70 percentage of the population of the world are using the internet.[1] This is due to the development and use of technology in recent past. We are currently living in the information era, which can be termed as a time where most of the human activities are information based. The main features of this age can be summarised as a rise in the number of information workers, a world that has turned out to be more open in the sense of communication and internationalization, the trans-outskirt stream of information. In the digital age, everyday life relies upon the utilization of technology.[2] Nowadays, technology has become an integral part of the life of human being. There is incipient advancement in the field of information and communication technology (ICT). Technology is very much affecting the living standard of everyone's life i.e. such as social media, biometric information for the identification, medical, economics, other official works, personal data saving and sharing, which may occur on the internet or non-internet data saving system. Every technology has some negative and positive aspect. With the rise of information technology, the issue of data protection and the right to privacy of an individual is a serious concern

---

1 Internet world stats *available at*: http://www.internetworldstats.com/stats.htm (visited on September 24, 2017).

2 J. J. Britz, Technology As A Threat To Privacy: Ethical Challenges to the Information Profession *available at* http://web.simmons.edu/~chen/nit/NIT%2796/96-025-Britz.html (visited on January 24, 2018)

in the digital domain. There are reported cases of hacking, unauthorized use of the personal data, misuse of identification information.

Human has great tendency to keep the things away from the public gaze. Privacy is one of the inalienable rights possess by the human-being. A natural right is not bestowed by the state but they inherited by human beings because they are human, these rights available equally to the individual irrespective of class, sex or orientation. Privacy is a broad term which means “A state in which one is not observed or disturbed by other people. The state of being free from public attention.”[3] Privacy has no definite parameters, and it has a diverse meaning for individual.[4] It allows each human being to be left alone in a core which is inviolable.[5] In liberal democratic systems, privacy creates a space distinct from political life, and allows personal autonomy, meanwhile safeguarding democratic freedoms of association and expression. Privacy is the heart of the freedom of dissent.

Marc Rotenberg has depicted the modern right to privacy as reasonable data hones. In his word "the rights and obligations identified with the accumulation and utilization of individual data". Further he describes that the distribution of rights is subject to information and the obligations are assigned to the information gatherers due to the exchange of the information among the individuals and the asymmetry of data with respect to information studies.[6]

Right to privacy is recognized in the various international instruments as well in regional instruments.[7] Right to privacy is a legal right in most of the democratic countries but as the constitutionally protected fundamental right. Some of the

---

3 *Oxford Advanced Learners Dictionary*, (Oxford University Press, 8th edition, 2015).

4 R. K. Chaubey, “*An Introduction to Cybercrime and Cyber Law”*, 929 (Kamal Law House, Calcutta, 2nd edition, 2012).

5 *Justice K.S. Puttaswamy (Retd.), And Another* v. *Union of India and Others.* AIR2017SC4161.

6 A. Allen& M Rotenberg, *Privacy Law and Society* (West Academic, New York 2016), *available at:* http://www.maria-online.com/electronics/Article.php?lg=en&q=Right_to_privacy (visited on 15 November 2017)

7 Universal Declaration of Human Right, 1948, International Covenant on Civil and Political Rights, 1966, International Convention on the Protection of the Rights of all Migrant Workers and Members of their Families, 1990, Convention on the Rights of Child 1989 recognize the same in respect of children, At the regional level, these rights are becoming enforceable. European Convention for the Protection of Human Rights and Fundamental Freedoms, 1950, American Convention on Human Rights, 1969, American Declaration of the Rights and Duties of Man, 1948.

developed countries of the world expressly recognize the right to privacy as fundamental right i.e. the Fourth Amendment of the Constitution of United States of America, Article 13 of the Constitution of Swiss Confederation, Article 23 of the Constitution of Russian Federation, Article 10and 13 of Constitution of Netherlands. In recent right to privacy declared as the fundamental right under the ambit of Article 21 of Indian Constitution by Apex Court. This paradigm shift brings in new judicial and legislative issue regarding the right to access online information and right to privacy which may threaten by the free flow of data.

Right to Privacy in India

The right to privacy does not explicitly mention under the Constitution of India and in any other statutes. The role of the judiciary is remarkable in this regard when the court interpreted the fundamental right to include the right to privacy. There is the tremendous development of constitutional jurisprudence of Article 21 of the Constitution of India which can be traced in various landmark judgements. The word “life and personal liberty” has given wide dimension by applying the golden rule of interpretation by the judiciary. Judiciary has recognized the right to privacy under the ambit of Article 21 and Article 14 of the constitution of India in landmark judgments. The earlier leading judgment acknowledged the right of privacy is *M P Sharma* v. *Satish Chandra, District Magistrate, and Delhi*[8], Further, followed by the *Kharak Singh* v. *State of Uttar Pradesh*[9] but the court refuses to recognise privacy as fundamental right. In the case of *M. P. Sharma*, the power of search and seizure is in any procedure of law, a primary power of the State for the assurance of public security and that power is essentially managed by law. Further it was held by the apex the constitution makers had no intention to bring privacy as the fundamental right analogous to Fourth Amendment in the Constitution of United States. So it is not justified to bring an entirely new fundamental right in the constitution. In the case, *Kharak Singh* v. *State of Uttar Pradesh's* case court discussed the matter of state surveillance as against the right to privacy. In a lengthy judgement, the court decided that "protection was not an ensured fundamental right". It may be held that Article 21 (right to life) is the store of residuary individual rights and perceived the

[8] (1954) SCR 1077.
[9] (1964) 1 SCR 332.

custom-based law right to privacy. The arrangement of Uttar Pradesh Police Regulation permitting domiciliary visits was called unlawful. It brought up that fundamental rights under privacy were totally unrelated and independent. In both the cases, the Supreme Court had stated that the right to privacy did not exist under the Indian Constitution. Further the issue of the right to privacy raised in a number of cases before the Supreme Court. In *R. Rajagopal* v. *State Of Tamil Nadu*, the Supreme Court expressly held that right to privacy or right to let alone is guaranteed by Article 21 of the constitution. Supreme Court recognized the right to privacy is as the fundamental right but by the less small bench than in earlier.[10]The issue of the right to privacy again raised in a recent case related to Aadhaar, the court declared that in paramount, right to privacy stands as the constitutionally protected fundamental right under Article 21 of Constitution of India.[11]

Right to Privacy and Data Protection

The data protection purpose of information security is to make a balance between individual privacy rights while still allowing data to be used for various purposes. Data protection is also known as data privacy or information secrecy. Another important thing is here Biometrics, which is the measurement and statistical analysis of people's physical and behavioural characteristics. The technology is used for identification, access control, or for authenticating individuals who are using the services.

The genesis of modern legislation in this field can be traced back to the first data protection law in the world enacted in the Land of Hesse in Germany[12] in 1970. This was followed by national laws in Sweden (1973)[13], the United States (1974)[14], Germany (1977)[15] and United Kingdom (1998)[16].There are guidelines of the Organisation for Economic Cooperation and Development (OECD) for the protection of data privacy, and transborder data flows of personal data freely

10 *Gobind* v. *State of Madhya Pradesh*, (1975) 2 SCC 148; *R Rajagopal* v. *State of Tamil Nadu* (1994) 6 SCC 632; *People's Union for Civil Liberties* v. *Union of India* (1997) 1 SCC 301.
11 *Supra note* 5.
12 Bundesdatenschutzgesetz (BDSG), 1990.
13 Data Protection Act (Act 289 of 1973).
14 US Privacy Act, 1974(5 U.S.C.).
15 Federal Data Protection Act, 1977.
16 Data Protection Act, 1998 (Chapter 29 1998).

specific rules covering the handling of electronic data and the European Convention for the Protection of Individuals about the Automatic Processing of Personal Data, 1981.

In India, there is no such specific law to govern the issue of data privacy. The protection of privacy governs by the Information Technology Act, 2000[17]. The AADHAAR (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016[18] is a legislative framework to back the scheme launched by the government. The essential guideline under the Act for biometric authentication is that everybody has unique fingerprints and an individual can be recognized by his or her physical or behavioural characters. Biometrics data additionally characterized as "Biometric Information" consists of a photograph, fingerprint, iris scan, and such other biological characteristics of a person which may be specified by protocols.[19] The primary objective of the scheme is to provide Unique Identification (UID) numbers to every resident of India having the demographic and

---

17 Section 6**6**E of the Information Technology Act, 2000 (Act 21 of 2000). Punishment for violation of privacy**.-** Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both

Explanation - For the purposes of this section--

(a) “transmit” means to electronically send a visual image with the intent that it be viewed by a person or persons;

(b) “capture”, with respect to an image, means to videotape, photograph, film or record by any means;

(c) “private area” means the naked or undergarment clad genitals, pubic area, buttocks or female breast;

(d) “publishes” means reproduction in the printed or electronic form and making it available for public;

(e) “under circumstances violating privacy” means circumstances in which a person can have a reasonable expectation that--

(i) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or

(ii) Any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.

18 Section 8, (1) The Authority shall ensure the security of identity information and authentication records of individuals. (2) Subject to the provisions of this Act, the Authority shall ensure confidentiality of identity information and authentication records of individuals.

19 Section 2(g), AADHAAR Act, 2016 (Act 18 of 2016).

biometric details.[20] The government has launched Aadhaar scheme, based on information technology, to give benefit to targeted beneficiaries. Data collected under the scheme is sensitive in nature as it contains biometric as well as demographic information of an individual. It gives rise to various issues of privacy of personal information. There is perceived danger to illegal use of information available in the form of data.

Research Problem

Privacy is one of the pertinent issues in the present scenario of information advancement around the world. India is also a significant player in information technology, having the vast network of internet and digital data users. Privacy in the digital world is a serious concern. People are saving their information in digital form in various platforms of a digital world. Biometric identification is also one of the techniques in digital data used for establishing the identity of the individual. Digital information of the individual is available at a single click and this particular fact highlights the need for data protection and protection of the right privacy of an individual. At present, the right to privacy stands as constitutionally protected fundamental right in India, as declared in *Justice K S Puttaswamy (Retd.), and another.* v. *Union of India and others* by the Apex Court of India[21]. The declaration of the right to privacy as the fundamental right will affect both individual and state. There is inevitable implication of a right to privacy on the social norms, government policies and national security. Government is promoting the digitalization of information through various scheme and programme. These policies are intended to encourage or in some cases force the citizen to utilize digital identity, digital

[20] Section 37, Whoever, intentionally discloses, transmits, copies or otherwise disseminates any identifiable data collected in the course of enrolment or authentication to any person not authorised by this Act or regulations made thereunder or in contravention of any agreement or arrangement entered into pursuant to the provisions of this Act, shall be punishable with imprisonment for a term which may extend to three years or with a fine which may extend to ten thousand rupees or, in the case of a company, with a fine which may extend to one lakh rupees or with both.

[21] *Supra note* 11

verification, digital mode of transaction etc. Right to Privacy of individual is likely to be in danger due to the mass collection and utilization of data. The present research focuses on the right to privacy and its nexus with data protection special reference to Aadhaar Act, 2016.

Objectives of the Study: The objectives of the study are:

1. To analyse the concept of privacy.
2. To study the recognition of privacy as a legal right.
3. To analyse the evolution of the right to privacy in India.
4. To analyse the nexus between the right to privacy and data protection under Aadhaar Act, 2016.
5. To conclude with the suitable suggestion to ensure the right to privacy through data protection.

Research Question

1. What is the meaning and scope of privacy?
2. Whether privacy is a recognized right?
3. What is role of Indian Judiciary in recognising privacy as fundamental right?
4. What is the nexus between right to privacy and data protection under Aadhaar Act, 2016?
5. How far right to privacy and data protection is recognized under Aadhaar Act, 2016?

Limitation of the Study

Due to time constraint, the present study is only confined to recent the Supreme Court judgment *Justice K S Puttaswamy (Retd.), and anothers.* v. *Union of India and others*[22] which declared the right to privacy as a fundamental right under Indian

[22] *Ibid.*

constitution and its impact on data protection under Aadhaar Act, 2016. Though this judgement has other implications on the various issue like homosexuality, family, RTI, which are not part of this study. The Aadhaar case in the Supreme Court reserved its verdict and the Court has not announced the judgement till the submission of the work. It would have some impact on right to privacy and data protection, which has not covered in the study.

Significance of the Study

India is a fast emerging economic power of the world. To ensure the growth rate Government of India has taken various Initiative like digital India, digitalization of data. Initiatives have been taken to promote the digitalization to ensure the transparency and there is the evolution of digital content consumption. But the move of the Supreme Court declaring the privacy as the fundamental right raised a debate in the academic field regarding the scope and extent of such individual right. The issue is relevant in regard to Aadhaar scheme and the debate about data protection under Aadhaar Act, 2016. The present study may help to authorities to formulate a sound policy for data protection. It may also help to the implementation machinery to mitigate the loopholes under the law in reference to misuse of data. The study is relevant in making a fine balance between the individual's right to privacy in reference to data protection under Aadhaar Act, 2016, as government policy to make compulsory use of Aadhaar Number to avail the services and benefits.

Project of the Study

The study divided into five chapters generating coordination and linkage between the main themes.

The first chapter entitled “introduction” has the brief background of the study. This chapter briefly describes the general components of the study, notion of privacy and its relationship with data protection, research problem, research question, significance and scope of the study. The issues, which have been discussed throughout the study, highlighted in this introductory chapter.

The second chapter entitled “review of the literature” which contains the analysis of the literature available on issue related to the theme of the study.

The third chapter entitled “research methodology” describe the methodology used in the study. The study is based on the analytical and descriptive mode of the research.

The fourth chapter entitled “detailed discussion” has the detailed study of the topic. The chapter divided into two-parts, first part contains the concept of the right to privacy followed by the legal recognition of privacy as the right at international, regional level and constitution of the various nations. It also discusses judicial approach towards the right to privacy at the international level and gradual development of privacy as the right in India and approach of the judiciary in India. Further, it contains its nexus with the security of the state. The second part has the discussion on the dimension of privacy in the Aadhaar Act, 2016, how the privacy protected in the Aadhaar Act, 2016, preceded by the introduction of the Aadhaar scheme. A study of cases has also been done in reference to protection of Information.

In the fifth chapter entitled “conclusion and suggestions” deals with the conclusions and suitable suggestions on the research topic. The major findings which have emerged from the study are presented in the light of the various objectives.

Chapter II

Review of literature

Review of literature is the important aspect of the research to study relevance of right to privacy and its nexus with the protection of information in the digital era. Review primarily focuses on the concept of privacy and its development and recognition of privacy as the right. Further study has been done on the importance of privacy in the digital world and recent development.

Brownlie and Goodwin (2007), stated that right to privacy is recognized in a various international instrument such as UDHR, ICCPR, even in the regional human right instruments recognised.[1] Kalin and Kunzli (2011), highlighted the content of origin of human right and detailed discussion about the international human right instrument and governing bodies such as human right commission, the complete focus on specific rights, right to life, protection of private life. According to him the protection of private life includes respect for privacy, respect of communities and respect at home, avoidance of unreasonable interference in one's life.[2]

Lloyd (2014), mainly discussed The Data Protection Act in the UK. The issue of privacy and surveillance in information-based society is discussed. Present society is surveillance society, privacy may be hurt by placing one under the surveillance which may be physical, psychological, and data-based. Need of time to protect and secure the flow of data of the individual. It may not be misused.[3] Rouland and Kohl (2012), had discussed the issue of internet misuse, data privacy, cybercrime, and information regulatory authorities in United Kingdom Laws as well as European Laws. According to him, there is Information Commissioner Office (UK) to regulate and control the information technology-based services under the Data Protection Laws. There shall be an equilibrium between the interest of individual and society, which include the efficient conduct of industry, commerce

---

1 Ian Brownlie CBE, QC and Guy S. Goodwin (eds.), *Basic Documents on Human Right*, (Oxford University Press Indian edition, 2007).

2 Walter Kalin and Jorg Kunzli, *The Law of International Human Right Protection*, (Oxford University Press, 2011).

3 Ian J. Lloyd, *Information Technology Law* (Oxford, edition 7, 2014).

and administration. It may vary society to society or within society subject to condition and use of data. [4]

Godbole (2015), observed that there are physical and environmental security, logical access control, metrics for the security, privacy in InfoSec. According to her, privacy and security are not the identical terms, privacy is a security issue, but security is necessarily not privacy issues.[5] Seth (2013)[6], analysed in detail about the law of technology in India, especially dealing with the Information Technology Act, 2000. Specially deals with the OECD, EU, IT Act. It also deals with data privacy law in USA and UK. Right to privacy in the modern era is fundamental to the dimensions of its protection of personal data, information privacy. A person using any website first time must go through the privacy rule on site. Chaubey (2012), stated that Privacy is the matter of concern in the digital era. Keeping in mind influence of the internet, it is imperative that India co-operate with the world community.[7]

Bansal(2013), viewed that there should be technology, capabilities, process and legal framework to respond the cyber event in near real time because economic security and national security going to totally depend upon on the information based system.[8]Ahmed and Booth (2016), analysed the provision related to protection of digital privacy in Jersey Island. This is primarily done by scrutinising the two key piece of legislation, The Employment (Jersey) Law 2003, and the Data Protection (Jersey) Law 2005. Neither of the laws have digital privacy provisions per se. This text is mainly related to digital privacy at the workplace, to ensure the privacy there should be a case study comprehensively done along with the examine the current legislation.[9]

---

4 Diane Rouland and Uta Kohl, *Information Technology Law,* (Routledge, edn. 4th 2012).

5 Nina Godbole, *Information System Security, Security Management, Metrics Frameworks and Best Practices* (Wiley, 2015).

6 Karnika Seth, *Computer Internet and New Technology Laws,* (Lexis Nexis, 2013).

7 R. K. Chaubey, *An Introduction to Cybercrime and Cyber Law* (Kamal Law House, Calcutta, 2nd edn. 2012).

8 S. K. Bansal, *Cyber Crime*, (A P H Publishing Corporation, New Delhi, 2013).

9 Ali Ahmed, David Booth, *The Digital Privacy Laws and Practices in the Jersey Island*, *PCS* 98 (2016) 163 – 168.

Naude (2014)[10], discussed the issue of data protection in South Africa. There is detailed discussion on the Protection of Information Act 2013. Purpose of the law is to give effect to the right to privacy and to follow the international standard in compliance with the data protection. According to study laws are good and is going to better with time. Rajvanshi and Singhal (2016)[11] viewed privacy concern adversely proportionate to the growth of electric transactions. Government is vigilant in making timely changes in the laws on the Data Protection but there is a need for a strong law on it. Datar (2017), observed that the right to privacy incorporates real privacy, informational privacy, and decisional autonomy. Humans do not know what the future holds for them. Irrespective of development of technology the individual's right of choice must be protected. The nine-judge bench has appropriately stressed the necessity of data protection laws—a project is consigned at a preliminary stage, to the Justice Srikrishna Committee.[12] Krishna (2018), determined that the constituent of the new security feature is a confession regarding lack of security information system of UIDAI.[13]

Sullivan (2013), analysed an emergent legal concept of digital identity as Government of U.S.A. move to put all federal government services online. The information that link the registered digital identification with individual is especially susceptible to non-accomplishment and deception. An accurate, functional, registered transaction identity, and its exclusive use, is vital to the one's ability to transact under the programme. In above perspective, the right to transaction identity is of a character that it cannot be denied without violating basic doctrines of liberty and justice.[14]

Weber (2015), observed that law relating to Data Protection and Privacy is subject to challenges in the modern technological era. While such technological

---

10 Adrian Naude, Data Protection in South Africa: The Impact of The Protection of Personal Information Act and Recent International Developments, *available at*: https://repository .up.ac.za/ bitstream/ handle/2263 /46094/ Naude_Data_2015.pdf? sequence=1 (visited on September 21, 2017).

11 Gargi Rajvanshi and Mayank Singhal, "Data Privacy Law And Growth Of E-Commerce: An Indian Perspective" *BLR* 1 (2016) *Available at:* www.manupatrafast.com (visited on 19 November 2017)

12 Editorial "Right to Privacy: A Right for the Future" *Indian Express,* August. 25, 2017.

13 Editorial "UIDAI's Post-Dated Cheque" *The Tribune,* January 20, 2018.

14 Clare Sullivan, Digital identity," Privacy and The Right to Identity in The United States Of America", *CLSR* 29, 348-358 (2013).

advancement is beneficial to society at large scale, yet these movements make issues for the security of a person's protection. The vibrant line of difference between diverse forms of information is blurring. There is an overlap of the content provided online. Public bodies also collecting the mass information of a person for various services through the means of administrative laws. Public bodies and private bodies are always ready to use available data. But use the use of such data is a matter of concern in relation to one's privacy. So data collecting bodies should ensure the protection of such big data.[15]

EIahi (2009), observed that in digital era no one has absolute access or control of all their existing personal information available online. This raises the issue of privacy and consent in this age which seems illusory and raises questions not only to the future form of cyberspace but also the political, social and economic interactions within it. The institution task with it are not well equipped in real sense to perform the similar role in virtual world as in physical world. There is prerequisite to develop cyberspace in conformity with the 21st century.[16]

Kak and Malik (2010), viewed that the silence in the bill (National Identification Authority Bill) regarding, who otherwise to request information under this law is a disturbing thing. Though provision on such an issue must be clear, as it is consider an important aspect of the privacy legislation. The terms 'security of state' 'national security' and 'interest of state' are used in various legislationa to justify the intrusion in privacy of one. But there is no uniformity on the issue of privacy in these legislation. Current need to bring uniform law on this issue to ensure right to privacy.[17]

Bird (2013), observed that enough privacy and enough security should be balanced. If biometric data are given for the one purpose it should be used only for that purpose though it is possible one set of data may be linked with another set

15 Rolf H. Weber, "The Digital Future E-A Challenge For Privacy?", *CLSR* 31 234-242(2015).
16 Shirin Elahi, "Privacy and Consent in the Digital Era", *ICTR*14, 113-118 (2009).
17 Amba Uttara Kak and Swati Malik, "Privacy and the National Identification Authority Of India Bill: Leaving Much To The Imagination", 3 (4) *NLR* 485 (2010).

intentionally or unintentionally. In a democratic setup, it is important to secure the interest of the individual.[18]

Sen (2015), stated that Aadhaar was initially started to curb the corruption and exclusion and poverty. Its main target was to deliver government services to the last men. When the Bill was introduced in the parliament there a major debate on the intrusion in privacy and security of such big data. According to the author in present BJP led government promoting the Aadhaar scheme at the peak in old days, they are in oppose to it. It is of the future think how much it is going to successful and secure. “The only thing that is guaranteed in the cyber-world is that no online database is ever secure."[19]

Diega (2016), observed that there is a need to develop some traditional concept of data protection, privacy and consumer protection in the era of the things of internet and cloud of things. In relation to Aadhaar act 2016, What is more, alarming is the unclear scope of the UIDAI's discretion in regulating the information to be collected and the exceptions to its sharing. Moreover, it is hard to understand why the judges' orders could regard photographs and demographic data, whereas the administration which usually acts secretly, has a blanket power to access also the biometric data. This paper is the output of ongoing research and future works should focus on the interaction between Things, cloud computing and AI technologies. According to the author further research should on the e-Health.[20]

Nayar (2011), viewed India is developing to towards the biological citizen by the means of Aadhaar identity, using the iris and fingerprint. While UIDAI declares that Aadhaar for the identity, not citizenship. But it has converted the Indian traditional society into socio-technical society. According to reports data may be used for the various services by the service provider but is not specifically who are particular service provider whom this data going to share. In the end the moral of the story

---

18 Stephanie J. Bird,” Security and Privacy: Why Privacy Matters” 19 *SEE*669–671. (2013)

19 Kalyani Menon Sen,” Aadhaar: Wrong Number, Or Big Brother Calling?” 11(2) *SLR* 85 (2015.

20 Guido Noto La Diego, "The Internet of Citizens: A Lawyer's View on Some Technological Developments in the United Kingdom and India”, 12 *IJLT* 53 (2016).

is in the age of multiveillance and function creep, guard your body with care. It is your passport to survival.[21]

Rajagopal (2012), highlighted that Civil Society initially invited to consult and give input for the proper working of Aadhaar. But this has not been come in practical due to some unavoidable issue and debate on the privacy by privacy advocates. According to him, there is a need for a renewed dialogue between the UIDAI and Civil Society on how they can work together to meet Aadhaar's pro-poor mission, while at the same time addressing the legitimate concerns regarding data privacy.[22]

Agrawal, Banerjee, Sharma (2017), observed that privacy concern in relation to Aadhaar protects much-heated debate in present. But the position in this regard of the government and UIDAI is not clear. Aadhaar may be one way of digitization but there a certain concern regarding the efficient design system to protect and control mass data. In the digital era, privacy protection does not mean non-sharing of the data. In return, one only want the protection of their data. Because there threat to identity theft due to the correlation of identities across the domain. There should be a third-party auditor to control the crucial decryption key. Aadhaar can be made safe with strong technology.[23]

There is a good amount of literature available on the issue of the right to privacy and its nexus with the information technology. Earlier studies done show that privacy is the pressing problem and it should be protected in the digital world. Since the Aadhaar Act, 2016 is new legislation come in force still the implementation of Act has not become standard, there is a research gap in reference to Aadhaar Act, 2016 and protection of information under the Act.

---

21 Pramod K Nayar, "'I Sing the Body Biometric' Surveillance and Biological Citizenship", *Economic and Political Weekly,* Vol. 47, No. 32 (August 11, 2012), pp. 17, 19-22 *available at*: http://www.jstor.org/stable/23251791 (visited on 4 February 2018).

22 Raju Rajagopal, "Aadhaar and Civil Society*", Economic and Political Weekly*, Vol. 47, No. 10 (March 10, 2012), p. 5, *available at*: http://www.jstor.org/stable/41419917 (visited on 4 February 2018).

23 Shweta Agrawal, Subhashis Banerjee, Subodh Sharma, "Privacy and Security of Aadhaar: A Computer Science Perspective", Vol. 52, Issue No. 37, 16 September 2017 *Economic and Political Weekly. available at*: http://www.jstor.org/stab le/41419917 (visited on 4 February 2018).

Chapter III

Research Methodology

In pursuing the present research work, the researcher has adopted the doctrinal method of research. As the title of the study mainly focused on the rights to privacy, which has multiple dimensions specifically in reference to the recent debate on data protection and privacy of an individual. The vulnerability of private data with the technological advancement in the present world is also the part of this debate. The researcher conducted a critical and analytical inquiry of the conceptualization of the notion of the privacy, politicization of the right to privacy in various international, regional and domestic instruments followed by the ongoing debate on its realization. In this regard it focuses on the recent apex court verdict recognised the right to privacy as fundamental right, use of data under the Aadhaar (targeted delivery of financial and other subsidies, benefits and services) Act, 2016.

Descriptive and analytical method of study applied during the present research work. The present work describes the scope and extent of the right to privacy. It also describes the role of the judiciary in the advancement of the jurisprudence of the right to privacy in India.

The analytical method of research is helpful in developing a critical approach to finding out facts and analysis it from the different perspective. This method has been used to critically analyse the provisions of The Aadhaar (targeted delivery of financial and other subsidies, benefits and services) Act, 2016 and the case of *Justice K S Puttaswamy (Retd.), and Anr.* v*. Union of India and Others*[1], in which the right to privacy was affirmed as a fundamental right. It is likely not possible to rely on a single approach. Both deductive and inductive methods of research have been used for this study. Keeping in notice the nature of research problem, both primary and secondary sources used for the research purpose.

In order to carry out the study, the help of various sources like the rulings and observations of Courts as found in law reports, statutes, committee reports, constituent assembly debates and parliamentary debates etc. have been taken.

---

1 AIR 2017 SC4161.

Further, all other formal and informal modes have been used to excerpt information from different quarters of society. The relevant information necessary for its completion has also been gathered from sources available in periodicals, articles in law journals, law reviews, newspapers, proceedings of the seminars, conferences, and online resources etc.

Chapter VI
Detail discussion

In the era of information technology, there are large amount of information is saved in cyberspace for various purposes. It may be personal information or other related information of the individual. But no technology is flawless as there is always threat to data stored. Privacy of data is here a matter of concern as it can be accessible through a single click if not protected properly. No one wants infringement of their right to privacy. Data Privacy is one of the aspect of right to privacy. The paradigm shift right to privacy as the fundamental right in India brings new ethical and juridical problems which are mainly related to data protection issues. Information technology industry is one of the fastest growing sectors in India. India is one of the major players in IT sector. Digital identification is one of the recent development of information technology. In India, a scheme, called Aadhaar scheme, is launched to give digital identity to an individual which explored the base for future of financial service and other essential services.

THE CONCEPT OF PRIVACY

Privacy has been derived from Latin word *privatus* meaning thereby "separated from the rest, deprived of something, where the office of the government has no role". The term privatus has been derived from term *privo* "to deprive". Privacy is the ability of individual or group of persons to separate self or information from other or to disclose it selectively. Privacy can be explained as an individual condition of life characterized by exclusion from publicity.[1]The concept follows from the right to be left alone which states that such a perception of privacy set the course for the passing of privacy laws in the United States.[2] Right to privacy consider as one of the fundamental rights in respect of the dignity of the individual, what is private should be private must not be disclosed without the prior permission

---

1 Neethling, J. and Potgieter, J.M. "*Neethling's Law of Personality"* 36 (Butterworths Durban,1996).

2 Privacy Act, 1974.

of person whom the information belongs. If there is something private to a person it may be sensitive in nature.

According to Gerety, privacy means an autonomy over the intimacies of identity of individual.[3] The right to privacy rest upon that "a certain private sphere of individual liberty will be kept largely beyond the reach of Government".[4] Respecting the individual's right to privacy means acknowledging the individual's freedom and existence as the human being. The obligation to respect a person's privacy is furthermore a prima facie duty. In other words, it is not an unqualified duty that does not allow for exceptions. Two examples can be given. Firstly, the police may encroach upon a criminal's privacy by spying or by seizing personal documents.[5] A government also has the right to collect private and personal information from its nations with the aim of ensuring order and harmony in society.[6] According to Cooley, privacy means "the right of one's person may be said to be a right of complete immunity; the right to be alone."[7] Here means right to live with privacy is an absolute right. It is free from the subject jurisdiction of the state, the state has no authority to break the ice in the life of the individual.

Privacy is an old concept. Its recognition can be traced in the ancient age. In the ancient age Greek philosopher Aristotle spoke about the diverse facets of human life, the public sphere of political affairs, *Polis* and personal sphere of political of political affairs, *okis*. This dichotomy provides recognition of privacy as "a confidential zone on behalf of the citizen".[8] This classification proved as basis for the restriction on government power to enter in the private sphere.

---

3 Shyam Sahu, Right To Privacy In India: Recent Trend, *available at*: http://snsah.blogspot.in/2013/03/by-adv_23.html (visited on 18 March 2018).

4 *Thornburgh* v. *American College of Obstetricians & Gynecologists*, 476 US 747, 772 (1986).

5 Mc. Garry, K. (1993). *The Changing Context of Information. An Introductory Analysis,* 178 (Library Association Publishing London 2nd edn.).

6 Ware, W.H "The New Faces of Privacy", *The Information Society*, 9 (3): 205 (1993).

7 Thomas Cooley, *Treatise On The Law Of Torts,(* 2nd edn. 1888).

8 Michel c James. "A Comparative Analysis of the Right to Privacy in the United States, Canada, Europe", *Connecticut Journal of International Law* vol. 29, issue 2 on page 261 (Spring 2014).

Further development of the right to privacy followed by the public and private distinction. Commentaries on the law of England, 1765[9] mentions distinction between private and public wrong. The private wrong concern with the infringement of the individual's right while public wrong affects the whole community for farmer remedy in civil law later tackle the criminal laws.

John Stuart Mill has also expressed that there should be preserve zone within which state authorities have no right to enter. This zone should be free from the interaction of the state.[10] John Stuart Mill also asserted his "harm principle" and said the state can control the actions of an individual to the extent that harms the other or to prevent the harm to other.[11] Further according to Mill "That principle is, that the sole end for which mankind are warranted, individually or collectively, in interfering with the liberty of action of any of their number, is self-protection. That the only reason for which power can be rightfully exercised over any member of the civilized community, against his will, is to avert harm to others."[12]The one is the sovereign over himself, over his own body and mind according to the Mill.

Right to Privacy implicitly recognized in the common law.[13] Privacy can be understood in its informational sagacity. It limits the ability of others to advance, disseminate, or use information about oneself. "Right to be let alone" it means the right to life will be enjoyed with it. Right to let alone embodied a manifestation of an inviolate personality. Freedom from the invasion in liberty.

The two theories of the literature of privacy are *reductionism* and *coherentism.* Reductionism is generally critical to privacy. The person advocating the theory is called a reductionist. They do not consider privacy as a separate concept.[14] There is nothing illuminating about the privacy and not distinctive in character. William

---

9 Online Version: Blackstone, William, Sir, 1723-1780. Commentaries on the laws of England. Boston: Beacon Press, [1962] (OCoLC) 654905622.

10 John Stuart Mill, *Of Liberty, Utilitarianism and Other Essay*, (Oxford University Press, Oxford, 2005).

11 Lakhwinder Singh, *Right to Privacy and Freedom of Media, 5 (*Satyam Law Publisher, edn. 1 2016).

12 John Stuart Mill, *Of Liberty*, *Utilitarianism and Other Essay*, 12-13 (Oxford University Press, Oxford, 2005).

13 Warren & Brandeis. "Right to Privacy" *HLR* 193. (1890).

14 Lakhwinder Singh, *Right to Privacy and Freedom of Media, 7 (Satyam* Law Publisher, edn.1 2016).

Prosser and Judith Jarvis Thompson, as reductionist see right to privacy in a very limited sense. According to them, the right to privacy is not a distinct right it is the part of the law of tort in four categories: - intrusion, public disclosure of private facts, false light and appropriation. According to Prosser "the law of privacy comprises four distinct kinds of invasion of four different interest of the plaintiff, which are tied together by the common name, but otherwise, have almost nothing in common except each represents an interference with the right of the plaintiff ' to be left alone'."[15] Coherentism, another group of theorist believe in the fundamental, distinctive and coherent character of various claims that have been called privacy interest and those who favour this are called coherentists.

Recognition of Privacy as Legal Right

Right to privacy is explicitly recognized in the various international, regional and national human right instrument. This is one of the basic rights recognised and protected by the law.

Right to privacy is recognized in the various international instruments as well under the local laws of multiple nations. Universal Declaration of Human Right, 1948[16], International Covenant on Civil and Political Rights, 1966[17], International Convention on the Protection of the Rights of all Migrant Workers and Members of their Families, 1990[18], Convention on the Rights of Child, 1989 recognizes the same in respect of children,[19]. At the regional level also these rights are becoming enforceable. European Convention for the Protection of Human Rights and

15 William L. Prosser, "Privacy"*, 48 CLR* 383, 389, (1960).

16 Article 12: no one shall be subject to arbitrary interference with the privacy, family, home, or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to protection of the law against such interference or attacks.

17 Article 17: No one shall be subjected to arbitrary or unlawful interference with the privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

18 Article 14: No migrant worker or member of his or her family shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home, correspondence or other communications, or to unlawful attacks on his or her honour and reputation. Each migrant worker and member of his or her family shall have the right to the protection of the law against such interference or attacks.

19 Article 16: of the Convention on the Rights of the Child, 1989.

Fundamental Freedoms, 1950[20], American Convention on Human Rights, 1969[21], American Declaration of the Rights and Duties of Man, 1948[22].

Privacy is broadly accepted concept recognized under the constitutions of different nations such as Constitution of the Islamic Republic of Afghanistan,[23] Constitution of The People's Democratic Republic of Algeria, [24] Constitution of the Azerbaijan Republic,[25] Constitution of Republic of Bulgaria,[26] Constitution of the Republic of

---

20 Article 8: (1) Everyone has the right to respect for his private and family life, his home and his correspondence. (2) There shall be no interference by a public authority with the exercise of this right except as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

21 Article 11 Right to privacy: 1. everyone has the right to have his honour respected and his dignity recognized; 2. No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation; 3. Everyone has the right to the protection of the law against such interference or attacks.

22 Article 10: Every person has the right to the inviolability and transmission of his correspondence.

23 Article 37: Freedom and confidentiality of correspondence, as well as communications of individuals, whether in the form of letter or via telephone, telegraph, as well as other means, shall be secure from intrusion. The state shall not have the right to inspect personal correspondence and communication unless authorized by the provision of law.

24 Article 39: The private life and the honour of the citizen are inviolable and protected by the law. The secrecy of private correspondence and communication, in any form, is guaranteed.

25 Article 32 Right for personal immunity: I. Everyone has the right to personal immunity. II. Everyone has the right to keep secret private or family life. It is prohibited to interfere with private or family life, except in cases established by law. Everyone has the right to be protected from unlawful interference in his or her private and family life. III. It is not allowed to obtain, keep, use and disseminate information about a person's private life without his or her consent. No one may be subjected to being followed, videotaped or photographed, tape recorded or subjected to other similar actions without his or her consent save activities in cases prescribed by law. IV. The state guarantees everyone the right to confidentiality with respect to correspondence, telephone communications, post, telegraph messages and information sent by other communication means. This right might be restricted, as specified by legislation, to prevent crime or to find out true facts when investigating criminal case. V. Everyone may become familiar with the materials collected in regards to him or her save in cases prescribed by law. Everyone has a right to demand correction or elimination of the information collected in regards to him or her, which does not correspond to the truth, is incomplete or collected through violation of the provisions of law. Article
33. Right for the sanctity of home: I. Everyone has the right for sanctity of his/her home.
II. Except cases specified by law or decision of law court, nobody has the right to enter private home against the will of its inhabitants.

26 Article 34: 1. The freedom and confidentiality of correspondence and all other communications shall be inviolable.
2. Exceptions to this provision shall be allowed only with the permission of the judicial authorities for the purpose of discovering or preventing a grave crime.

Croatia,[27] Constitution of the Federal Democratic Republic of Ethiopia,[28] Constitution of the Sovereign Democratic Republic of Fiji,[29] Constitution of Finland,[30] Constitution of Georgia,[31] Basic law for the Federal Republic of

[27] Article 36: The freedom and privacy of correspondence and all other forms of communication shall be guaranteed and inviolable. Restrictions necessitated by the protection of national security and the conduct of criminal prosecution may be prescribed solely by law.

[28] Article 26 Right to Privacy: 1. Everyone has the right to privacy. This right shall include the right not to be subjected to searches of his home, person or property, or the seizure of any property under his personal possession.
2. Everyone has the right to the inviolability of his notes and correspondence including postal letters, and communications made by means of telephone, telecommunications and electronic devices.
3. Public officials shall respect and protect these rights. No restrictions may be placed on the enjoyment of such rights except in compelling circumstances and in accordance with specific laws whose purposes shall be the safeguarding of national security or public peace, the prevention of crimes or the protection of health, public morality or the rights and freedoms of others.

[29] Article 24 Right to privacy : (1) Every person has the right to personal privacy, which includes the right to—
(a) Confidentiality of their personal information;
(b) Confidentiality of their communications; and
(c) Respect for their private and family life.
(2) To the extent that it is necessary, a law may limit or may authorise the limitation of, the rights set out in subsection (1).

[30] Article 10 - The right to privacy: Everyone's private life, honour and the sanctity of the home are guaranteed. More detailed provisions on the protection of personal data are laid down by an Act.
The secrecy of correspondence, telephony and other confidential communications is inviolable. Measures encroaching on the sanctity of the home, and which are necessary for the purpose of guaranteeing basic rights and liberties or for the investigation of crime, may be laid down by an Act.
In addition, provisions concerning limitations of the secrecy of communications which are necessary for the investigation of crimes that jeopardise the security of the individual or society or the sanctity of the home, at trials and security checks, as well as during the deprivation of liberty may be laid down by an Act. .

[31] Article 20: 1. Everyone’s private life, place of personal activity, personal records, correspondence, communication by telephone or other technical means, as well as messages received through technical means shall be inviolable. Restriction of the aforementioned rights shall be permissible by a court decision or also without such decision in the case of the urgent necessity provided for by law.
2. No one shall have the right to enter the house and other possessions against the will of possessors, or conduct search unless there is a court decision or the urgent necessity provided for by law.

Germany.[32] Constitution of South Africa,[33] Constitution of Italian Republic,[34] Constitution of Japan,[35] Constitution of Kuwait,[36] Constitution of Republic of Namibia,[37] Constitution of Poland,[38] Constitution of Netherlands,[39] Constitution of

---

32 Article 10- Privacy of correspondence, posts and telecommunications.
(1) The privacy of correspondence, posts and telecommunications shall be inviolable.
(2) Restrictions may be ordered only pursuant to a law. If the restriction serves to protect the free democratic basic order or the existence or security of the Federation or of a *Land*, the law may provide that the person affected shall not be informed of the restriction and that recourse to the courts shall be replaced by a review of the case by agencies and auxiliary agencies appointed by the legislature.

33 Article 14 privacy: Everyone has the right to privacy, which includes the right not to have— (a) their person or home searched; (b) their property searched; (c) their possessions seized, or (d) the privacy of their communications infringed.

34 Article 15: Freedom and confidentiality of correspondence and of every other form of communication are inviolable. Limitations may only be imposed by judicial decision stating the reasons and in accordance with the guarantees provided by the law.

35 Article 21(2): No censorship shall be maintained, nor shall the secrecy of any means of communication be violated.

36 Article 39: Freedom of communication by post, telegraph and telephone and the secrecy thereof shall be guaranteed; accordingly censorship of .communications and disclosure of their contents shall not be permitted except in the circumstances and manner specified by law.

37 Article 13 Privacy: (1) No persons shall be subject to interference with the privacy of their homes, correspondence or communications save as in accordance with law and as is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the protection of health or morals, for the prevention of disorder or crime or for the protection of the rights or freedoms of others.
(2) Searches of the person or the homes of individuals shall only be justified:
(a) where these are authorised by a competent judicial officer;
(b) in cases where delay in obtaining such judicial authority carries with it the danger of prejudicing the objects of the search or the public interest, and such procedures as are prescribed by Act of Parliament to preclude abuse are properly satisfied.

38 Article 49: The freedom and privacy of communication shall be ensured. Any limitations thereon may be imposed only in cases and in a manner specified by statute.

39 Article 10: 1. Everyone shall have the right to respect for his privacy, without prejudice to restrictions laid down by or pursuant to Act of Parliament. 2. Rules to protect privacy shall be laid down by Act of Parliament in connection with the recording and dissemination of personal data. 3. Rules concerning the rights of persons to be informed of data recorded concerning them and of the use that is made thereof, and to have such data corrected shall be laid down by Act of Parliament.
Article 13: 1. The privacy of correspondence shall not be violated except in the cases laid down by Act of Parliament, by order of the courts. 2. The privacy of the telephone and telegraph shall not be violated except, in the cases laid down by Act of Parliament, by or with the authorisation of those designated for the purpose by Act of Parliament.

Russian Federation[40], Constitution of Swiss Confederation[41] and Constitution of United States of America.[42]

Judicial Approach

Although privacy is not strictly a political question, we can use the political question doctrine as a useful analogy. In particular, the current constitutional right of privacy reflects the same view of judicial supremacy that has been allowed to erode the political question doctrine. The Court's recognition of a constitutional right of privacy began in *Griswold v. Connecticut*[43] where the Court struck down a law prohibiting the use of contraceptives, even by married couples. The Court ruled that the statute violated "a zone of privacy" created by the "penumbras" that gave "life and substance" to the specific guarantees in the Bill of Rights. In outlining this zone of privacy, the Court stated that even though some rights are not specifically enumerated in the Constitution, they are nonetheless "peripheral" to various freedoms in the Bill of Rights.

Although Griswold may have initially appeared to link the constitutional protection of sexual activity to married couples, *Eisenstadt* v.*Baird*[44] removed any such linkage. In *Eisenstadt*, the Court extended Griswold's holding to include right to beget or bear child to free from the governmental intrusion. Any unwarranted interference in this fundamentally affecting the individual's right to bear or beget children by the married or individual. As Justice Brennan declared, "[i]f under Griswold the distribution of contraceptives to married persons cannot be prohibited, a ban on distribution to unmarried persons would be equally impermissible." This

---

40 Article 23: 1. Everyone shall have the right to the inviolability of private life, personal and family secrets, the protection of honour and good name.
2. Everyone shall have the right to privacy of correspondence, of telephone conversations, postal, telegraph and other messages. Limitations of this right shall be allowed only by court decision.

41 Article 13: (1) Every person has the right to respect for his or her private and family life, home, and secrecy of mail and telecommunication.
(2) Every person has the right to be protected against abuse of personal data.

42 Fourth Amendment: 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 or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

43 381 U.S. 479 (1965).

44 405 U.S. 438 (1972).

decision marked a shift from privacy as "freedom from surveillance or disclosure of intimate affairs," to privacy as "the freedom to engage in certain activities" and "to make certain sorts of choices, free of interference by the state."[45]

The Court, in *Carey* v. *Population Services International*[46], reiterated that "the reasoning of Griswold could not be confined to the protection of rights of married adults." Carey extended the right of privacy to minors engaging in consensual sexual behaviour by overturning a state statute that banned the distribution of contraceptives to minors as part of a state policy against teen pregnancy. The Carey Court saw the right of privacy, as protected by the Due Process Clause of the Fourteenth Amendment, include right to choice and decisional privacy. In *Roe* v. *Wade*[47], the Court held that the right of privacy recognized in the previous contraception cases was "broad enough to cover the abortion decision." Later, in Planned Parenthood of *Southeastern Pennsylvania* v. *Casey*[48], which reaffirmed Roe, Justice Kennedy elaborated the right to privacy. The central idea of Fourteenth Amendment is protection of liberty by not infringing the right of personal choices. Matter of choices is intimate to privacy. At the core, liberty is the right to define one's own concept of life. The latest noteworthy pronouncement from the Supreme Court of USA on the right of privacy came in *Lawrence* v. *Texas*[49] which held that a state statute criminalizing same-sex sodomy violated the Fourteenth Amendment's Due Process Clause. In Lawrence, the Court applied the right of privacy to hold that a Texas statute prohibiting people of the same sex from engaging in certain sexual conduct violated the Due Process Clause. Justice Kennedy's opinion recognized that the Court's earlier decision in Eisenstadt had established that the right to make certain decisions regarding sexual conduct extended to all adults, regardless of marital status. But in Lawrence, the Court now gave explicit recognition to a right of sexual intimacy, which it had been unwilling to make in previous cases.[50] Even though the Court seventeen years earlier in

---

45 Michael J. Sandel," Moral Argument and Liberal Toleration: Abortion and Homosexuality", 77 *CLR* 521, 527-28 (1989).

46 431 U.S. 678, 687 (1977).

47 410 U.S. 113, 155 (1973).

48 505 U.S. 833, 851 (1992).

49 539 U.S. 558, 578 (2003).

50 H.J. Hermann, "Pulling the Fig Leaf off The Right of Privacy: Sex and the Constitution",54 *DLR* 909, 928-930 (2005).

Bowers v. *Hardwick*[51] had found that there was not a fundamental right of homosexuals to engage in sodomy, based upon a lack of history or tradition in protecting such a practice, the Lawrence Court found just the opposite type of history and tradition, ruling that sodomy statutes offended an individual's right to privacy. Consequently, in the wake of Lawrence, there is no longer any question as to whether a right to sexual privacy exists. The only question is what specific aspects of sexual privacy can or cannot be regulated.[52] In his dissent, for instance, Justice Scalia predicted that the next logical step in the reasoning of Lawrence would be the legalization of same-sex marriage.

Right to privacy is explicitly recognized in the United Kingdom under the Human Right Act 1998.[53] Earlier, English law was reluctant to recognize a general law of the personal privacy. Right to privacy is in the debate since 1961 by the introduction of the Private Member Bill by Lord Bancroft, which was followed by the Younger Committee's Report, has the view that there is a need for the change of law in reference to unlawful surveillance by the means of technical devices. *Chemical* v. *Falkman Ltd*[54] (1982) Lord Denning stated that right to privacy is a fundamental right as the right to freedom of expression. *Kaye* v. *Robertson Glidewell LF*[55] Glidewell said "It is well known that in English law there is no right to privacy, and accordingly there is no right of action for breach of a person's privacy. The facts of the present case are a graphic illustration of the desirability of Parliament

---

51 478 U.S. 186, 190 (1986).

52 Williams v. Att'y Gen'l of Ala., 378 F.3d 1232, 1233 (11 th Cir. 2004) (addressing the constitutionality of an Alabama statute regulating the distribution of sexual devices, including the specific issue of whether the right to sexual privacy includes the right to use sexual devices).

53 Article 8- Right to respect for private and family life:
(1)Everyone has the right to respect for his private and family life, his home and his correspondence.
(2)There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

54 [1982] QB 1.

55 [1991] FSR 62.

considering whether and in what circumstances statutory provision can be made to protect the privacy of individuals".[56]

The English law of the privacy governed by the Law of Torts, Breach of Confidentiality and Law of Trespass before Human Right Act, 1998. *Hickman* v. *Maisey*[57] where the claimant relied on trespass to prove invasion of privacy. In this case, the claimant owned and occupied land on which for a fee he allowed a racehorse trainer to train a horse. The defendant, a racing tout, observed the horses from a highway that crossed the claimant's land, with a view to gain information about the horses. The claimant files a suit in trespass for damages and an injunction. He was awarded damages in addition to the Injunction.[58] Law of breach of confidentiality is one of the points to protect the invasion of privacy. When it comes to action on the breach of the personal information, then cause of action arising in the breach of confidence is the strongest. *Coco* v. *A.N. Clark* [59] set the parameter of the action on the basis of the breach of confidentiality, the information must be quality of confidence importing obligation to maintain confidentiality and there must be unauthorised use of the information to determine the case. Further stated by the court that breach privacy in public places does not attack the right to privacy.

Evolution of Right to Privacy in India

The element of privacy can be marked out in the ancient text of Hindus, Hitopadesh mentions that certain matter of worship, sexual characteristics, and the family matter should be protected.[60] But this cannot be a positive law it may be positive morality.

---

56 Sam Makkan, Privacy, Parliament & The Judiciary *available at*: http://www.actnow.org.uk/media/articles/Privacy_Parliament_and_the_Judiciary.pdf (visited on 8 April 2018)

57 [1900] 1 QB 752.

58 Current Position of Privacy Law in UK' (Lawteacher.net, April 2018) *available at:* <https://www.lawteacher.net/free-law-essays/constitutional-law/current-position-of-privacy-law-in-uk-constitutional-law-essay.php?vref=1> (visited on 8 April 2018).

59 [1968] F.S.R. 415.

60 Right to Privacy the Indian Perspective' (Lawteacher.net, March 2018*) available at*: <https://results.searchlock.com/?vref=1> (visited on30 March 2018).

The notion of privacy was a trump against the state interferences with personal freedom was first expressed in the Constitution of India Bill drawn up in 1895 by the authors whose identity is not well established. The text of the Bill was that *"Every citizen has in his house an inviolable asylum".* It was a simple articulation of the classic English privacy notion that for every man his home is his castle and the state could not invade without the legal procedure, which is fair.[61] Further in 1925, The Commonwealth of India Bill was drawn up for self –governance, Mahatma Gandhi, Bipin Chandra Pal and Mrs Sarojini Naidu were among the members of the committee under the Chairmanship of Sir Tej Bahadur Sapru. The Bill recognised the privacy as the right "*Every person shall have the fundamental right to liberty of person and security of his dwelling and property".* Here ambit of privacy extends to personal liberty and security for one's property apart from one's home. The Nehru (Swaraj) Report, 1928 three years later the Indian National Congress constituted a committee under the Chairmanship of Motilal Nehru to draw up a plan for Swaraj (self-rule) for India. Renowned freedom fighter Netaji Subhash Chandra Bose was a member of this Committee. This Committee placed 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 recognised in Anglo-Saxon Jurisprudence is quite evident in this connotation. [62]

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 set up under the Chairmanship of Acharya J B Kripalani. Various members of the CA sent their views on what fundamental rights guarantees should be incorporated in the Constitution and why. On the Right to Privacy, K T Shah wanted the following (December 1946): *"Every citizen of India has and is hereby guaranteed the security of his person, papers, property, house or effects against unreasonable searches or seizure."* K M Munshi's note called

---

61 Venkatesh Nayak, Understanding the Right to Privacy, History, Jurisprudence and Implications for India's RTI Regime *available at:* http://cic.gov.in/sites/default/files/2012/R2Privacy-Venkatesh.pdf (visited on 10 may 2018).

62 Evolution of Right to Privacy in India, *available at*: http://www.rtifoundationofindia.com/evolution-right-privacy-India (visited on 10 may 2018).

for this draft 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 recognised for citizens and one for everybody including non-citizens. Harnam Singh called for 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 had elaborated it more favouring 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*."[63] Dr Ambedkar wanted to fit in a strong safeguard against violation of the right to privacy but at the same time allowing State action where required under strict monitoring by Judicial Authority. In March 1947, the Sub Committee 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*". Later in April, the final draft was 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 or 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 recognised 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 threw a spanner in the works. They argued that guaranteeing the right to privacy would impede law enforcement and the criminal prosecution of conspirators who will most likely be captured in their dwellings. They also pointed out that the Constitution of USA did not explicitly guarantee the right to privacy to its people.[64] So the Advisory Committee on

63 Address by Dr Ambedkar in constituent assembly (March 1947).

64 *Supra note* 62

Fundamental Rights dropped the proposal to recognise the right to privacy as a fundamental right. However, the right to property and protection for the person of the individual were included as separate fundamental rights in Article 19 and 21. Much later the right to privacy was downgraded to a constitutional right and inserted as Article 300A in the Constitution. So the Constitution was written up and enforced in 1950 without an explicit recognition of the individual's privacy as a fundamental right.[65]

Though the right to privacy does not explicitly mention under the Constitution of India and other statutes it is recognized by the judiciary. There is the tremendous development of constitutional jurisprudence of Article 21 of the constitution of India which can be traced in various landmark judgements. The word “life and personal liberty” has given wide dimension by applying the golden rule of interpretation by the judiciary. Judiciary has recognized the right to privacy under the ambit of Article 21 and Article 14 of the constitution of India in landmark judgments. The earlier leading judgment acknowledging the right of privacy is *M P Sharma* v. *Satish Chandra, District Magistrate, Delhi*[66]*.* Further, it followed by *the Kharak Singh* v. *State of Uttar Pradesh*[67]*.* In the case of *M. P. Sharma* court held that the power of search and seizure in any law is intervening power of state to ensure the social and national security. The Constitution makers not thought fit to put privacy as fundamental right analogous to Fourth Amendment in the Constitution of U.S.A. it not justified to put new fundamental right by strained construction.[68]

Further *Kharak Singh* v. *State of Uttar Pradesh's* case[69] brought to court the matter of state surveillance as against the right to privacy. In this case provisions of the Uttar Pradesh Police Regulations had permitted domiciliary visits at night and secret picketing of Singh’s house, tracing his movement and periodic inquiries by officers. The writ petition was filed before the Supreme Court saying that this was an infringement of his fundamental rights. A six-judge bench scrutinized the issue

---

65 *Supra note* 61.
66 (1954) SCR 1077.
67 (1964) 1 SCR 332.
68 *M. P. Sharma and Others* v. *Satish Chandra, District Magistrate, Delhi, and Others* (1954) SCR 1077.
69 *Supra note* 67.

of surveillance and regulations validity governing the Uttar Pradesh police. The main contention was whether surveillance under the Uttar Pradesh Police Regulations constituted an infringement of the fundamental rights as guaranteed by the Constitution. Police authorities contended that the regulations did not encroach on upon fundamental freedoms and even if they did, they served as reasonable restrictions for the general public's interests and for the efficient discharge of police duty. In a significant judgment, the court ruled that “privacy was not a guaranteed fundamental right”. It, however, held that Article 21 (right to life) was the repository of residuary personal rights and recognised the common law right to privacy. Though, the provision of Uttar Pradesh Police Regulation allowing domiciliary visits was called unconstitutional. It is acknowledged that fundamental rights under privacy were mutually exclusive and self-contained. Justice Subbarao was a dissenting voice who, however, said that even though the right to privacy was not recognised as a fundamental right, it was essential to personal liberty under Article 21. He also held all surveillance to be unconstitutional. In both the cases, the Supreme Court had stated that the right to privacy did not exist under the constitution of India.

In *Gobind,* under regulation 855 and 856 of state Police regulations, a history sheet was opened against the petitioner who had been placed under surveillance. Three judges bench adverted the judgment of *kharak Singh.* Supreme Court recognized right to privacy as the fundamental right but by the smaller bench than earlier.[70] New jurisprudence of right to privacy has been developed from the mid 1970's though judiciary started the recognition of privacy as the fundamental right but the verdict which was delivered by the judiciary were of the smaller bench which had no such effect as the earlier decision still prevailing over that decision as they are of the larger bench decision.

In view of the Apex Court in *Smt. Maneka Gandhi* v. *Union of India & Anr*[71] the term ‘personal liberty' in Article 21 covers various rights and some are recognized as fundamental rights. Court also lays down triple test for law to intrusion in one’s

---

70 *Gobind* v. *State of Madhya Pradesh*,(1975) 2 SCC 148; *R Rajagopal* v. *State of Tamil Nadu* (1994) 6 SCC 632; *People’s Union for Civil Liberties* v. *Union of India* (1997) 1 SCC 301.

71 1978 SCR (2) 621.

personal liberty that there should be prescribed procedure which withstand the test of Article 19 and in conformity with Article 14. The law laid down the procedure of intervention in liberty must be fair and reasonable. In view of Apex Court "*The fundamental right to life and personal liberty has many attributes and some of them are found in Article 19. If a person's fundamental right under Article 21 is infringed, the State can rely upon a law to sustain the action, but that cannot be a complete answer unless the said law satisfies the test laid down in Article 19(2) so far as the attributes covered by Article 19(1) are concerned."*

Malak Singh case[72] dealt with the Police Rules, section 23, which deals with the surveillance on the habitual offender. Court held that it recognize the surveillance of the habitual offender. Further the issue of the right to privacy raised in a number of cases before the Apex Court., In *R. Rajagopal* v. *State Of Tamil Nadu,* the Supreme Court explicitly held that right to privacy or right to let alone is assured by Article 21 of the Indian Constitution. In *Naz Foundation* Right to privacy held to protect a "private space in which man may become and remain himself.[73] One need a place to be free from social control where he is free to show real of himself.

The issue of the right to privacy over again raised in Supreme Court in a recent case related to Aadhaar, where the three-judge bench had referred the matter of privacy for consideration to larger bench in respect of *MP Sharma* and *Kharak Singh* case. The reference has been disposed of declaring right to privacy as a fundamental right. Court held that decisions in *M.P Sharma* and *Kharak Singh* extend to which not upholding that privacy is protected by the Constitution of India stand over-ruled*.* The right to privacy is an inherent part of the right to life and personal liberty in the ambit of Article 21. It is a part of the freedoms guaranteed by Part III of the Indian Constitution. "In paramount, right to privacy stands as the constitutionally protected fundamental right."[74]Though it is a negative right put a positive obligation on the state to secure the secrecy of its subjects and not to intrude in their life.

---

72 *Malak Singh* v. *State Of Punjab and Haryana*, (1981) 1 SCC 420.

73 *Naz Foundation* v. *Govt. of NCT Delhi and Others*, WP(C) No.7455/2001 July 2, 2009.

74 AIR 2017 SC4161.

This is one of the landmark judgments which is going to change the direction of Indian society as well as the Indian legal setup. It is going to be a milestone in the recent future development. The Puttaswamy is historic and landmark verdict of time and one of the important verdict delivered by the Apex Court in the field of civil right. It will impact interconnection between privacy and transparency and free speech and privacy.[75] The government was here of the view that there is no right to privacy to an individual in the light of *M.P.Sharm case* and *Kharak Singh case.* Further, it was contended that constitution maker has no such intention to give the right to privacy otherwise they would clearly mention in the constitution. The court adverted the arguments of the government and overrule two earlier judgements which form the crux of government's arguments *MP Sharma v. Satish Chandra and Kharak Singh* v. *State of Punjab* observing that jurisprudence of right to privacy exists from 1975, has the legal position. This judgement reflects the gradual development of the privacy in the recent era. There are six different view which is slightly different and there is overlap also.[76]

Justice Chelameswar held that privacy has the three facet in it, response, sanctuary, intimate decision. Justice Nariman of the view that privacy is the right to move freely, this is explicitly framed in the realm of the private sphere. Justice Bobde focused on the right to seclusion both physical and mental. Justice Kaul, right to control the dissemination of personal information.[77] At last, Justice Chandrachud observed that *"Privacy has distinct connotations including (i) spatial control; (ii) decisional autonomy; and (iii) informational control. Spatial control denotes the creation of private spaces. Decisional autonomy comprehends intimate personal choices such as those governing reproduction as well as choices expressed in public such as faith or modes of dress. Informational control*

---

75 Gautam Bhatia, The Supreme Court's Right to Privacy Judgement, *available at*: http:// www.livelaw.in/supreme-courts-right-privacy-judgment-foundations/ (visited on 5 April 2018).

76 The Supreme Court's Right to Privacy Judgment – II: Privacy, the Individual, and the Public/Private Divide *available at*: https://indconlawphil.wordpress.com/2017/08/28/the-supreme-courts-right-to-privacy-judgment-ii-privacy-the-individual-and-the-publicprivate-divide/ (visited on 5 March 2018).

77 *Ibid.*

empowers the individual to use privacy as a shield to retain personal control over information pertaining to the person."[78]

M.P.Sharma was correct in refusing Article 20(3) not analogues to Fourth Amendment of America correct. Justice Bobde held "*M.P. Sharma is unconvincing not only because it arrived at its conclusion without enquiry into whether a privacy right could exist in our Constitution on an independent footing or not, but because it wrongly took the United States Fourth Amendment- which in itself is no more than a limited protection against unlawful surveillance – to be a comprehensive constitutional guarantee of privacy in that jurisdiction.*"[79] Further, it overrules the *kharak Singh* case in the broader sense, resurrecting the dissenting view of the Justice Subba Rao, Justice Chandrachud observed about privacy and dignity *"Individual dignity and privacy are inextricably linked in a pattern woven out of a thread of diversity into the fabric of a plural culture."*[80]

The idea of noticed and consent also highlighted in reference to the information of individual though the court was at the refusal to understand the privacy in the relational term. In terms of Justice Kaul, who stated the principle in so many words, *"The State must ensure that information is not used without the consent of users and that it is used for the purpose and to the extent, it was disclosed."* [81] Everyone has the right to control the personal information. With the notice and consent information can be used by the authorised person or body.

In the end, privacy infringement under Article 21 must satisfy the proportionality and legitimate purpose and fair and reasonable procedure must be guaranteed. The real thing is to prove the necessity of law must be proved in democratic setup to avoid the abuse of procedure. It is upon the state to prove that law in need and there is a minimal infringement of rights. Burden on the state that privacy is not infringed. There is need to set the standard for balance between the individual right to privacy and the interest of the state.

---

78 *Ibid.*
79 *Supra note* 74.
80 Para 168, AIR 2017 SC4161.
81 Para 70, AIR 2017 SC4161.

Right to privacy as a fundamental right has opened the various topic of debate i.e. sexual orientation, biometric encryption, health information, marital life, reproductive right etc. a person needs privacy in their life to enjoy their life own at own will and merit. Privacy as the fundamental right has put an obligation on the state to secure the privacy of individual no intrusion in one's life should be done without the procedure of law.

Right to Privacy and National Security

According to Helen Keller "Security is mostly a superstition. It does not exist in nature. Life is either a daring adventure or nothing"[82] Security is topic of debate since the terrorist attacks on 11 September 2001 in the USA and 26 September 2011 in India. Security is an issue that encounters every day.[83] Security in any matter needs to be considered at the earlier stage then it will not pose a problem at the end. It means it is the matter of security arise in any matter of law this subject must become into consideration first any other aspect.

The right to privacy time and again must be balanced against the state's persuasive interests, including the promotion of public safety and improving the class of life.[84] A fundamental right is available against the state but the state has some responsibility one of them is national security, if there is a conflict between fundamental right and national security, later will prevail. This concept is highlighted in the Indian constitution under Article 19.[85] Article 19 clause (1) (a) gives a citizen to freedom of speech and expression but clause (2) restrict it on the

---

82 Quoted in Rich Colman, Security is Mostly a Superstition*, available at*: http://calmanknight.com/security-is-mostly-a-superstition/ (visited on 22 April 2018).

83 Essay on National Security vs. the Right to Privacy *available at:* https://www.bartleby.com/essay/National-Security-vs-the-Right-to-Privacy-P3WYUNZVJ (visited on 21 April 2018).

84 Right to Privacy: Constitutional Rights & Privacy Laws, Available *At: https*://www.livescience.com/37398-right-to-privacy.html. Tim Sharp. (visited on 17 February 2018).

85 Article 19. Protection of certain rights regarding freedom of speech etc
(1) All citizens shall have the right (a) to freedom of speech and expression;
(2) Nothing in subclause (a) of clause (1) shall affect the operation of any existing law, or prevent the State from making any law, in so far as such law imposes reasonable restrictions on the exercise of the right conferred by the said sub-clause in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality or in relation to contempt of court, defamation or incitement to an offence.

several grounds one of the securities of the state. But the right to privacy declared as the fundamental right under the ambit of Article 21. In the name of security of state individual's right to privacy should not be infringed. The state should try to maintain a balance between national security and individual's right to privacy. The state should not allow the executive machinery to access them in the life of one and data related to them, which is not strictly consonance with the national security.

Supreme Court in *Gobind* v. *State of Madhya Pradesh*[86] held that privacy can be violated with the sanction of law. In this view privacy is not absolute it can be infringed by the process of law. This is the natural extension of the Article 19(2), where the government can deprive his citizen of certain freedom on the ground stated in the Article 19(2). In *Peoples union for civil liberties* v. *Union of India*[87] the right of government authorities to interpret, in the interest of the sovereignty, the integrity of the state, the message transmitted or received by telegraph, was challenged in the context of wiretapping.[88] Supreme Court held that tapping a person's telephone line violation of his right to privacy unless it is done in gravest of grave circumstances. This may be a restriction on the fundamental right but must use this power in restraint manner.

The term Privacy and Security are contradictory in nature as one cannot absolutely achieve without the overriding the other. Right to privacy now stands as the fundamental right in India under the ambit of the Article 21 read with 19(1) here situation is different from the USA where separate right under the Constitution of USA. Individual Privacy and National Security both need to be protected

86 (1975) SCC (Cri) 468.

87 (1997) 1 SCC 318.

88 Section 5 (2) of the Indian Telegraph Act, 1885: (2) On the occurrence of any public emergency, or in the interest of the public safety, the Central Government or a State Government or any officer specially authorised in this behalf by the Central Government or a State Government may, if satisfied that it is necessary or expedient so to do in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of an offence, for reasons to be recorded in writing, by order, direct that any message or class of messages to or from any person or class of persons, or relating to any particular subject, brought for transmission by or transmitted or received by any telegraph, shall not be transmitted, or shall be intercepted or detained, or shall be disclosed to the Government making the order or an officer thereof mentioned in the order: Provided that the press messages intended to be published in India of correspondents accredited to the Central Government or a State Government shall not be intercepted or detained, unless their transmission has been prohibited under this sub-section].

simultaneously. But the national security is much important than individual privacy. One has right to life and personal liberty and freedom which is protected by the state. It is right to live without the control of the government but the government has the obligation of larger interest to make sure that person not doing any act which is a threat to the security of the state. Recently government agencies are much focusing on the surveillance in day to day business to ensure the national security. There is need to strike the balance between the right to privacy and national security.

In view of John Lock, it is impossible for men to remain in Free State of Nature. This natural utopia is shattered by the realization that each person cannot secure his liberty for himself and also not to punish transgressors on his own. By this insight men enter into an obligatory commitment to civil society and submit his will in demand of common good, mankind sacrifices freedom for less free majority rule.[89] Here the argument is that whether men live in a total Free State of Nature or Minimal Government is necessary. Men should be controlled through the limited government maintaining the balance between security and liberty, in view of the Lock limit should be imposed on the liberty of men in the interest of others liberty, it should be relatively reasonable.

In this reference to national security and right to privacy integral part of liberty, reasonable nexus should be maintained because no right is absolute. But the state has no licence to put an unreasonable restriction on the liberty. George Orwell's description of a totalitarian society in 'Nineteen Eighty-Four' in which the citizenry is subjected to a high degree of control and intrusive surveillance might not only be a metaphoric concept but closer to present-day realities. As the 'Orwellian metaphor' has underlined, the public and the social realm cannot exist without protecting privacy and freedom.[90]

With information communication technology touching various facet of daily life, the objective understanding of its implication on 'Privacy' are limited, include volume,

---

89 Gordon Neal Diem, Locke, Hobbes and the Free Nation *available at:* http://www.freenati on. org/a/f53d2.html (visited on 25 April 2018).

90 Dionysios Politis, *Socioeconomic and Legal Implications of Electronic Intrusion*, 131 (London: IGI Global, 2009).

magnitude, complexity and persistence of information. This ICT revolution has created a paradigm challenge to the security of privacy as there is a possibility to misuse the data gathered and stored. This ICT has become the challenge for the security of the state. There is tension increasing between the Principle of Security and Principle of Privacy. The threats of internal extremism, terrorism, radical insurgency, threats from rogue nations and asymmetric threats from non-state actor shave all resulted in deepening and intensification of security discourses across the full spectrum of the political, economic, social and legal landscape.

The pressing question to maintain the balance between national security and right to privacy, with growing threat of terrorism and mounting national security concerns, the law enforcement agencies have also extended their arsenal of methods to snoop through the digital packets transiting through the networks and gather records and data, carry out audio and visual surveillance and track movements. The digital surveillance has become far more pervasive and intrusive and is perceived as natural a manifestation of problems of modern times, somewhat relegating the issue of privacy to incongruity. The resolution of the debate on privacy versus national security rests on the extent to which national security concerns outweigh the rights of citizens to privacy of their associations and communications and on the extent to which democratic concepts such as privacy and freedom can be accommodated within a larger security conception and framework.[91]

Right to Privacy and Aadhaar Act, 2016

The Aadhaar project is run by the Unique Identification Authority of India (UIDAI), established by a resolution of Planning Commission, Government of India vide notification number[92], which collects personal and biometric data such as Fingerprints, Facial Photographs, and Iris Scans, and issues 12-digit Individualized Identity Numbers. Aadhaar was initially meant to be voluntary, targeted at eliminating fraud in government welfare scheme and giving people a form of

---

91 Richard H. Rovere and Gene *Brown, Loyalty and Security in a Democratic State*,354 (New York: Ayer Company Publishers, 1977).

92 *Vide Notification No*. A-43011/02/2009- Admin. I dated the 28th January 2009.

identification. The government had started a programme to collect the demographic and biometric information of the citizens for digital identification, without any legislative framework, and without close-fitting how information is to be used, who has access to the information and what are the safeguards, including legal and technical, to protect the information from going into the in the wrong hand.[93]

On 3rd December 2010, The National Identification Authority of India Bill was introduced in the upper house of the parliament. Further referred by the Lok Sabha speaker to the standing committee on finance a week later. When the NIDAI Bill of 2010 failed to obtain the majority of parliament for the passing of Bill, the government took another route that was the introduction of Bill as the money bill with the certain changes, Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Bill, 2016 in March 2016. This was done to evade the interference of the Upper House of the Parliament has no say on the money bills. But the.[94] Article 110 of the Constitution of India defines Money Bill[95], Article

---

93 Hem Raj Singh, AADHAAR Act is it Fraud on the Constitution?, *available at*: http://www.web.lawyersupdate.co.in/cover-story/aadhaar-act-is-it-fraud-on-the-constitution/ (visited on 10 April 2018).

94 *Ibid.*

95 Article 110 in The Constitution Of India:
110. Definition of Money Bill
(1) For the purposes of this Chapter, a Bill shall be deemed to be a Money Bill if it contains only provisions dealing with all or any of the following matters, namely
(a) the imposition, abolition, remission, alteration or regulation of any tax;
(b) the regulation of the borrowing of money or the giving of any guarantee by the Government of India, or the amendment of the law with respect to any financial obligations undertaken or to be undertaken by the Government of India;
(c) the custody of the Consolidated Fund or the Contingency Fund of India, the payment of moneys into or the withdrawal of moneys from any such Fund;
(d) the appropriation of moneys out of the Consolidated Fund of India;
(e) the declaring of any expenditure to be expenditure charged on the Consolidated Fund of India or the increasing of the amount of any such expenditure;
(f) the receipt of money on account of the Consolidated Fund of India or the public account of India or the custody or issue of such money or the audit of the accounts of the Union or of a State; or
(g) any matter incidental to any of the matters specified in sub clause (a) to (f)
(2) A Bill shall not be deemed to be a Money Bill by reason only that it provides for the imposition of fines or other pecuniary penalties, or for the demand or payment of fees for licences or fees for services rendered, or by reason that it provides for the imposition, abolition, remission, alteration or regulation of any tax by any local authority or body for local purposes
(3) If any question arises whether a Bill is a Money Bill or not, the decision of the Speaker of the House of the People thereon shall be final

109 of the Constitution makes it binding that the Money Bill be presented only in the Lok Sabha. The Money Bill contains the matters such as imposition, abolition, remission, alteration or regulation of any tax. Here the important point clause 1(c) (d) (e) of Article 110, which are related to regulation of Consolidated Fund of India including payment of money into or the withdrawal from such fund, appropriation of the fund, dealing in expenditure to charge on the fund. Because of the preamble of the Aadhaar Act 2016. By means of computer technology, a person can collect information about consumers, and trace their activities. Computer software can coalesce this data and prepare it for use by direct marketing companies, leading institutions, insurance companies, and credit bureaus.[96]

The Aadhaar (Target Delivery of Financial and Other Subsidies Benefits and Services) Act, 2016 (Aadhaar Act 2016) is a legislative framework to backed the scheme launched by the government. The main object of the scheme is to provide every resident of India Unique Identification (UID) numbers having the demographic and biometric detail of the individual. However, the Aadhaar Act of 2016 and subsequent notifications and licensing agreements enlarged the scope of the project, making Aadhaar enrolment mandatory for people to access a range of necessary services and benefits including government subsidies, pensions and scholarships. It has also been linked to services such as insurance, banking, telephone, and the Internet.

The Aadhaar (targeted delivery of financial and other subsidies, benefits and services) Act, 2016 is “An Act to provide for, as a good governance, efficient, transparent, and targeted delivery of subsidies, benefits and services, the expenditure for which is incurred from the Consolidated Fund of India, to individuals residing in India through assigning of Unique Identity Numbers to such individuals and for matters connected therewith or incidental thereto.”[97]

---

(4) There shall be endorsed on every Money Bill when it is transmitted to the Council of States under Article 109, and when it is presented to the President for assent under Article 111, the certificate of the Speaker of the House of the People signed by him that it is a Money Bill.

96 Privacy *available at:* https://www.encyclopedia.com/social-sciences-and-law/law/law/ right-privacy (visited on 10 April 2018).

97 The preamble of the Aadhaar Act, 2016.

In short, the Act aims at to bring the good governance and transparency in the services concerning the PDS of which expenditure incurred from the Consolidated Fund of India. The correct identification of targeted beneficiaries for delivery of various subsidies, services, grants, wages and other social benefits schemes which are funded from the Consolidated Fund of India has become a challenge for the government. Failure to establish a secure identification is the major problem in delivering the services. In absence of a credible authentication system of identifying the beneficiaries, it is difficult to ensure that the servicers reach to intended beneficiaries. Through the Aadhaar Numbers, it is felt that the process of enrolment, authentication, and security in delivering can be ensured efficient and the accurate person will get the benefit of services.

Protection of Data under Aadhaar Act, 2016

The Act consists of the 59 sections divided into VIII chapters of a different head. Chapter one is preliminary , chapter two is related to, enrolment, chapter third authentication, chapter four, establishment of UIDAI, chapter five grant, accounts and audit and annual report, chapter six, protection of information, chapter seven offences and penalties and chapter eight miscellaneous and there are regulation also framed by the authority under the power given by the said act.[98]

Privacy of an individual is the matter of concern in the Aadhaar scheme as it collects the biometric and demographic information of the individual. This

[98] The relevant provision relating to the protection of information (power of authority to make regulation) under Section 54 is as follows:
(1) The Authority may by notification make regulations consistent with this Act and the rules made thereunder, for carrying out the provisions of this Act.
(2) In particular, and without prejudice to the generality of the foregoing power, such regulations may provide for all or any of the following matters, namely:
(t) the manner of accessing the identity information by the Aadhaar number holder under the proviso to sub-section (5) of section 28;
(u) the manner of sharing the identity information, other than core biometric information, collected or created under this Act under sub-section (2) of section 29;
(v) the manner of alteration of demographic information under sub-section (1) and biometric information under sub-section (2) of section 31;
(w) the manner of and the time for maintaining the request for authentication and the response thereon under sub-section (1), and the manner of obtaining, by the Aadhaar number holder, the authentication records under sub-section (2) of section 32;
(x) any other matter which is required to be, or may be, specified, or in respect of which provision is to be or may be made by regulation.

information is sensitive in nature. It is the duty of UIDAI ensure the privacy of data collected from the individual it must not go to the wrong hand. Chapter VI of the Act deals with the protection of information along with Aadhaar (data security) Regulation, 2016.

While Section 29(4) of the Aadhaar Act prohibits the publication of Aadhaar number or biometric details, it has no provision in place to notify persons whose information has been leaked. The Section also fails to include data authentication records or Metadata related to Aadhaar based transactions within its domain, indirectly legitimising abuse of such records. In fact, the Aadhaar (Sharing of Information) Regulation 2016, allows for such information to be published, provided the Aadhaar number is redacted or blacked out (Rule 6). In the off-chance that an individual may find that Aadhaar data has been leaked, one can approach the UIDAI Contact Centres. However, one will not be able to approach the court, as, under Section 47(1) of the Act, recourse for the breach of the Aadhaar Act lies only with the UIDAI. This directly vitiates the principle of independence, impartiality and neutrality, basic to the rule of law.

Section 28[99] deals with the security and confidentiality of information. But there are no measures given how security and confidentiality will be maintained. There is the

[99] Section 28-Security and confidentiality of information:
(1) The Authority shall ensure the security of identity information and authentication records of individuals. (2) Subject to the provisions of this Act, the Authority shall ensure confidentiality of identity information and authentication records of individuals. (3) The Authority shall take all necessary measures to ensure that the information in the possession or control of the Authority, including information stored in the Central Identities Data Repository, is secured and protected against access, use or disclosure not permitted under this Act or regulations made thereunder, and against accidental or intentional destruction, loss or damage. (4) Without prejudice to sub-sections (1) and (2), the Authority shall— (a) adopt and implement appropriate technical and organisational security measures; (b) ensure that the agencies, consultants, advisors or other persons appointed or engaged for performing any function of the Authority under this Act, have in place appropriate technical and organisational security measures for the information; and (c) ensure that the agreements or arrangements entered into with such agencies, consultants, advisors or other persons, impose obligations equivalent to those imposed on the Authority under this Act, and require such agencies, consultants, advisors and other persons to act only on instructions from the Authority. (5) Notwithstanding anything contained in any other law for the time being in force, and save as otherwise provided in this Act, the Authority or any of its officers or other employees or any agency that maintains the Central Identities Data Repository shall not, whether during his service or thereafter, reveal any information stored in the Central Identities Data Repository or authentication record to anyone: Provided that an Aadhaar number holder may request the Authority to provide access to his identity information excluding his core biometric information in such manner as may be specified by regulations.

scope for misuse of information. There is no punishment provided in the Section in case of a breach. Further in section 29[100] restriction on the sharing of the information without the consent of Aadhaar holder and purpose specified by him or her. But the clause 4 of section gives a room to publish the information without the consent. There is a possibility that in the name of necessity or urgency sensitive may be going in wrong hands. Right to life includes the individual's control over the body and information. When in regard to such information scope will be given to disclose or publish the information it is against the individual's right to live without the interference in their life.

Section 30 states that biometric information deemed to be sensitive personal information under the Information Technology Act, 2000. Further, it limits the extent of Information Technology Act, 2000 as it in addition to Aadhaar Act, not derogatory to Act of 2016. Sensitive personal data means such personal information as may be prescribed by the Central Government in consultation with professional bodies as it may deem fit.[101] Under this sensitive personal data or information include password, financial information, health information, sexual orientation, biometric information[102]

Section 43-A of Information Technology Act, 2000 deals with compensation for failure to protect data.[103] This section imposes the penalty in way of compensation

---

100 Section 29 Restriction on sharing information: (1) No core biometric information, collected or created under this Act, shall be— (a) shared with anyone for any reason whatsoever; or (b) used for any purpose other than generation of Aadhaar numbers and authentication under this Act. (2) The identity information, other than core biometric information, collected or created under this Act may be shared only in accordance with the provisions of this Act and in such manner as may be specified by regulations. (3) No identity information available with a requesting entity shall be— (a) used for any purpose, other than that specified to the individual at the time of submitting any identity information for authentication; or Security and confidentiality of information. Restriction on sharing information. (b) disclosed further, except with the prior consent of the individual to whom such information relates. (4) No Aadhaar number or core biometric information collected or created under this Act in respect of an Aadhaar number holder shall be published, displayed or posted publicly, except for the purposes as may be specified by regulations.

101 Section 43-A Information Technology Act, 2000.

102 IT Act 43A Consulting available at: http://www.crystalonnet.com/services/g overnance-risk- and-compliance-services/it-act-43a-consulting. (visited on 22 April 2018).

103 43A Compensation for failure to protect data:
Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to

on the body corporate which is dealing or handling any sensitive personal data. If there is negligence in maintaining the security and wrongful loss or gain caused to a person. UIDAI is also a body corporate as per the Section 11(2) of the Aadhaar Act, 2016.[104] Authority may be held responsible for the breach of duty under the IT Act, 2000 but it is in addition to Aadhaar Act not derogatory to it.

Section 33, of Act 2016, the disclosure of information in certain cases, by the order of the court not below the District Court information of identity, authentication record may be disclosed. The proviso of the subsection (1) provides that opportunity of hearing to be given to the authority. Here question arises on the proceeding why this right has been given to authority. Authority has a role to protect and safeguard the data gathered. Information belongs to a person, that person has no right to participate in the hearing. Aadhaar number holder should have this right along with the authority. If Aadhaar Card to consider as the property, the sole owner of the property is Aadhaar Card holder, not authority, it is only a service provider in this regard. The owner has the all right to use property in which manner he wants to.

Section 37 provides the penalty for disclosing the information, which is three years imprisonment or fine up to ten thousand rupees or in case of company fine up to one lakh rupees. The penalty is very less in reference to sensitive information. It should be strict.

---

pay damages by way of compensation to the person so affected. Explanation. -For the purposes of this section,-
(i) "body corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities;
(ii) "reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit;
(iii) "sensitive personal data or information" means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.].

104 Section 11 (2): The Authority shall be a body corporate by the name aforesaid, having perpetual succession and a common seal, with power, subject to the provisions of this Act, to acquire, hold and dispose of property, both movable and immovable, and to contract, and shall, by the said name, sue or be sued.

Aadhaar (Data Security) Regulations, 2016 formulated under the power given by the clause (p) subsection (2) section 54(v) of the act, 2016, contains total 10 regulation in regard to data security. Regulation 3, measures for ensuring information security:

(1) The Authority may specify an information security policy setting out inter alia the technical and organisational measures to be adopted by the Authority and its personnel, and also security measures to be adopted by agencies, advisors, consultants and other service providers engaged by the Authority, registrar, enrolling agency, requesting entities, and Authentication Service Agencies.

(2) Such information security policy may provide for:—

(a) Identifying and maintaining an inventory of assets associated with the information and information processing facilities;

(b) Implementing controls to prevent and detect any loss, damage, theft or compromise of the assets;

(c) Allowing only controlled access to confidential information;

(d) Implementing controls to detect and protect against virus/malware;

(e) A change management process to ensure information security is maintained during changes;

(f) A patch management process to protect information systems from vulnerabilities and security risks;

(g) A robust monitoring process to identify unusual events and patterns that could impact security and performance of information systems and a proper reporting and mitigation process;

(h) Encryption of data packets containing biometrics, and enabling decryption only in secured locations;

(i) Partitioning of CIDR network into zones based on risk and trust;

(j) Deploying necessary technical controls for protecting CIDR network;

(k) Service continuity in case of a disaster;

(l) Monitoring of equipment, systems and networks;

(m) Measures for fraud prevention and effective remedies in case of fraud;

(n) The requirement of entering into non-disclosure agreements with the personnel;

(o) Provisions for an audit of internal systems and networks;

(p) Restrictions on personnel relating to processes, systems and networks.

(q) The inclusion of security and confidentiality obligations in the agreements or arrangements with the agencies, consultants, advisors or other persons engaged by the Authority.

(3) The Authority shall monitor compliance with the information security policy and other security requirements through internal audits or through independent agencies. (4) The Authority shall designate an officer as Chief Information Security Officer for disseminating and monitoring the information security policy and other security-related programmes and initiatives of the Authority

Here is the regulatory authority has the discretion in formulation measures, as the word *may* use in the regulation "the authority may specify" in clause (1) of the Regulation 3. Data gathered in Aadhaar scheme is very sensitive in nature and how much discretionary power has been given to authority. There should be provision for mandatory obligation to ensure the information security. There is no specific privacy policy formulated by the UIDAI though it should be there under the regulation 3(2) which fix the areas concerning the policy. Regulation 4, security obligation of the personnel, based on the principle of natural justice, imposing a duty to comply with the information policy and duty to not breach confidence. If the act of personnel in ultra vires of the policy, action will be taken after giving the opportunity of hearing.[105]

[105] Regulation 4.-Security obligations of the personnel: (1) The personnel shall comply with the information security policy, and other policies, guidelines, procedures, etc. issued by the Authority from time to time. (2) Without prejudice to any action that may be taken under the Act, personnel may be liable to an action in accordance with procedures specified by the Authority for this purpose: Provided that no such action shall be taken without giving the concerned personnel a reasonable opportunity of being heard.

Security obligation of the service provider, etc given in Regulation 5.[106] The service provider consultants, agencies shall ensure the protection of data gathered, confidentiality of data. Ensure the handling of the data by limited expert personnel in confidence.

Regulation 6, Audits and inspection of service providers, etc. — (1) All agencies, consultants, advisors and other service providers engaged by the Authority, and ecosystem partners such as registrars, requesting entities, Authentication User Agencies and Authentication Service Agencies shall get their operations audited by an information systems auditor certified by a recognised body under the Information Technology Act, 2000 and furnish certified audit reports to the Authority, upon request or at time periods specified by the Authority. (2) In addition to the audits referred to in sub-regulation (1), the Authority may conduct audits of the operations and systems of such entities or persons, either by itself or through an auditor appointed by the Authority.

Here in this Regulation, there is the appointment of the Auditor for the working of authority. The auditor will be appointed in compliance with the Information Technology Act, 2000. Section 18 (i) of IT Act, 2000[107] has the provision for the

---

106 Regulation 5-Security obligations of service providers, etc. : The agencies, consultants, advisors and other service providers engaged by the Authority for discharging any function relating to its processes shall:
(a) ensure compliance with the information security policy specified by the Authority;
(b) periodically report compliance with the information security policy and contractual requirements, as required by the Authority;
(c) report promptly to the Authority any security incidents affecting the confidentiality, integrity and availability of information related to the Authority's functions;
(d) ensure that records related to the Authority shall be protected from loss, destruction, falsification, unauthorised access and unauthorised release;
(e) ensure confidentiality obligations are maintained during the term and on termination of the agreement;
(f) ensure that appropriate security and confidentiality obligations are provided for in their agreements with their employees and staff members;
(g) ensure that the employees having physical access to CIDR data centres and logical access to CIDR data centres undergo necessary background checks;
(h) define the security perimeters holding sensitive information, and ensure only authorised individuals are allowed access to such areas to prevent any data leakage or misuse;
(i) Where they are involved in the handling of the biometric data, ensure that they use only those biometric devices which are certified by a certification body as identified by the Authority and ensure that appropriate systems are built to ensure the security of the biometric data.

107 Section 18 (i) specifying the terms and conditions subject to which auditors may be appointed and remuneration to be paid.

appointment of the Auditor as it is the power of controller appointed under the section 17 of IT Act. But clause (2) of the regulation 6 gives authority may appoint the auditor on its behalf. There is conflict in both the clause. Regulation 7 of data security regulation talks about the maintenance of confidentiality.[108] Right to Privacy is an intrinsic part of liberty has the vital role in the right to life. Everyone has the right to enjoy their personal life with the interference of other. By the increase of use of information communication technology, the privacy of the individual is up to some extent come under the threat. In India Right to Privacy stands as the fundamental right under the shadow of article 21 of the constitution. Right to privacy and national security one of the topic of debate, there is need to strike the balance between them. In reference to Aadhaar act, 2016 there is need to revisit the legislation in the current scenario.

Case Study on the Aadhaar scheme in reference to protection of privacy

Data gathered under the Aadhaar Scheme is the property in possession of an organization (CDRI) ownership lies with the Aadhaar card holder, the organization must give assurance to the person of protection of data. According to Times of India, Maharashtra accepted that their 3 lakh base data was lost with the PAN. This incident occurred when the IT department was uploading biometric information and PAN data to UIDAI centralized servers in Bangalore (then Bangalore) due to the accident of the hard disk. In fact, the data was being uploaded and was encrypted using strong algorithms, and when headquarters data was downloading, they could not decrypt it. Therefore many applicants who complained about this were asked to re-register for this. Later, the state (Mumbai) IT department said that the data relates to the people of Mumbai, and the lost data is being completely secured, if

[108] Regulation 7-Confidentiality: All procedures, orders, processes, standards and protocols related to security, which is designated as confidential by the Authority, shall be treated as confidential by all its personnel and shall be disclosed to the concerned parties only to the extent required for giving effect to the security measures. The nature of information that cannot be shared outside the Authority unless mandated under the Act includes, but not limited to, Information in CIDR, Technology details, Network Architecture, Information security policy and processes, software codes, internal reports, audit and assessment reports, applications details, asset details, contractual agreements, present and future planned infrastructure details, protection services, and capabilities of the system.

you have 'keys and multiple clues' then only can be opened is. The state ensures that the data is safe but such issues have already raised serious concerns.[109]

In the recent case[110], MS Dhoni's wife, Sakshi Dhoni, tweeted the law and justice ministry and electronics and IT ministry about the base data of MS Dhoni, taken by CSC e-Governance Services India Limited 37. CSC E-Governance Services India Ltd posted a picture of a screenshot of MS Dhoni's base data as well as MS Dhoni fingerprint scanning. The shocking thing was that the electronics and IT minister also liked the tweet and the photo of MS Dhoni's fingerprint was scanned by the CSC Agency. Later, UIDAI took strong action and blacklisted CSC e-Governance Services India Limited for next 10 years. In spite of all these rules and regulations for sharing the information of the partner company, raise the issue whether any confidentiality has been left and whether it ensures that the base data is in the right hands or not. According to sources in Indian Express, for the first time, the NDA government has admitted that the base data was leaked to the public domain for the first time. Although the government was ignoring the fact that the base is a sensitive data and by saying it assures us that the base is completely safe and it cannot be easily violated. Since the base database is the largest database management, information loss or security breach of the base database can be a serious threat to India.[111] In a shocking incident, Jharkhand's old age pension scheme has compromised the names, addresses of the beneficiaries, base number and information of bank accounts, programming error on the website created by Directorate of Jharkhand Social Security. It should be noted that Jharkhand Government has more than 1.6 million pensioners, out of which 1.4 million have given birth to their bank accounts with their base accounts to avail the

---

109 Maharashtra Loses Data of 3 Lakh UID Cards. *available at:* http://timesofindia.indiat imes.com/city/mumbai/Maharashtra-loses-data-of-3-lakh-UIDcards/articleshow/1968 71 25.cms. (visited on 23 April 2018)

110 MS Dhoni's Aadhaar Details Leaked, Wife Sakshi Complains to Ravi Shankar Prasad. *available at:*http://www.hindustantimes.com/cricket/ms-dhoni-s-personal-info-from-aadhar-card-form-leakedwife-sakshi-complains/story-8M4B7ZabHIu8cAcWhKuIzH.ht ml. (visited on 29 March 2018).

111 The government admits your Aadhaar data has been leaked *available at:* http://www.newind ianexpress.com/nation/2017/mar/31/government-admits-your-aadhaar-datahas-been-leaked-1588027.html. (visited on 31 March 2018).

direct bank transfer for their monthly pension. Since the information of all the citizens can be accessed independently by logging on to the website, in this case, the serious risk of adding the Aadhaar card to the different card's capabilities has increased.

In a shocking incident, Jharkhand's old age pension scheme has compromised the names, addresses of the beneficiaries, base number and information of bank accounts, programming error on the website created by Directorate of Jharkhand Social Security.[112] It should be noted that Jharkhand Government has more than 1.6 million pensioners, out of which 1.4 million have given birth to their bank accounts with their base accounts to avail the direct bank transfer for their monthly pension. Since the information of all the citizens can be accessed independently by logging on to the website, in this case, the serious risk of adding the Aadhaar card to the different card's capabilities has increased. In similar cases in Kerala, the database of more than 35 lakh pensioners has been leaked from the Kerala State Pension Department. Those 35 lakh pensioners added their base number and bank account according to the "base benefit transfer" scheme. The service pension website had placed any names, addresses, phone numbers, bank account numbers, base numbers and photographs of anyone to download an excessive violation of the Aadhaar Act. Apart from this, the Pension ID was also used to draw information, and the data was pulled from the website after the news was stirred.[113]

In Chandigarh, the Department of Food and Supplies and Consumer Affairs shared the UID number of people on their website. It was said that the details of the person's ration card, date of birth, husband and wife were displayed on their public domain. In fact, the Ministry of Water and Sanitation, which is considered as one side of the Swach Bharat Mission, has also publicized the base details of

---

112 Details of over a million Aadhaar numbers published on Jharkhand govt, *available at*: http://www. hindustantimes.com/india-news/in-massive-data-breach-over-a-million-aadhaarnumbers-published-on-jharkhand-govt-website/story-EeFlScg5Dn5neLyBzrkw1I.html. (visited on 29 April 2018).

113 Aadhaar leak: 35 lakh people in Kerala have their personal data breached. *available at*: http://english. manoramaonline.com/news/kerala/2017/04/25/aadhaar-leak-people-Kerala-personal data-breached.html. (visited on 25 April 2018).

citizens with details such as Citizen ID number, ration card number and their caste status.[114] However, due to various cases of data leakage from the government domain, the Central Government has recently broadcast a set of 27 DUs and 9 DOTs on data results and instructed to encrypt sensitive data with legal consequences. Apart from this, each department has been asked to review their public domain to see if there is any personal data on the display and to allocate an officer who should be responsible for data protection.[115]

Right to privacy one of the inalienable rights naturally inherited by the human being. Privacy has the gradual development with the passing of time and peripheral of privacy depends upon the society and person's personal idea of living. In India privacy not specifically mention under the Constitution of India but Supreme Court held that privacy is the fundamental right under the ambit of Article 21. Privacy has the close nexus with the digital world as it is wide open to access information. Everyone wants to protect their information from authorizing intrusion by anybody. Aadhaar scheme is product development of information technology in India. It aimed at creating of digital identity of the individual for accurate identification of the individual by biometric detail. But no technology is defect free there is always a threat that information may go in to wrong hand. Aadhaar Act, 2016 has the provision in reference to privacy under chapter VI, Protection of Information. There is need to revisit the act in light of recent development.

---

114 Now, Swach Bharat portal leaks Aadhaar details online. *available at*: http://www.newind ianexpress.com/nation/2017/apr/25/now-swachh-bharat-portal- leaks-aadhaardetails-online-1597359--1.html. (visited on 25 April 2018).

115 Centre brings in new safeguards following cases of Aadhaar data leaks on government *available at*: http://economictimes.indiatimes.com/articleshow/58952785.cms?utmsou rce=contentofinterest&ut m_medium=text&utm_campaign=cppst. (visited 2 May 2018).

Chapter V

Conclusion and Suggestions

Privacy notoriously has many different aspects depending on the different people and different culture. The idea of privacy mainly includes the “right to be let alone”. At the core, privacy protects the self, whether decline access of other to your person, avoid control and observation by the others or hold back information about yourself.[1] Privacy is a process by which individuals set the criteria and boundaries in their life. It means a limitation of access. The concept of the privacy seems to be elusive. The notion can be seen in term of one’s expectation. Intrusion in one’s life violate the privacy of individual depends upon the condition expected, unusual, offensive or shocking but there is no general concept can be formulated related to the notion of privacy.

Right to privacy is an inherent and inalienable human right recognised under various international, regional and national instruments. It is the duty of the State to ensure the privacy of the individual in order to serve one’s dignity and person. Now, Right to Privacy recognized as the fundamental right in India under the ambit of Article 21 of Constitution. Privacy is the core of human dignity. Privacy has normative as well descriptive function. At a normative level, privacy sub-serves eternal values upon which the guarantees of life and personal liberty is founded. At a descriptive level, protection proposes a bundle of qualifications and interests which lie ordered liberty. Like the other fundamental rights given under the part III of the Constitution of India legitimate right to privacy is not absolute. The law which infringes security must be sensible and reasonable. In light of judgments delivered by the Apex Court of India, the invasion on right to life and personal liberty should have fair and legitimate expectation. Privacy protects one’ self-administration and sees the limit of the individual to control basic bits of life.

Informational privacy is one of the aspects of privacy. It is closely related to the right to liberty. There is threat to privacy in the age of Information Communication Technology not only from the state as well as from non- state actors. There is need

---

[1] Leslie P. Francis and John G. Francis, *Privacy What Everyone Needs to Know,* 2, (Oxford University Press, New Delhi 2017).

to strike balance between the state interest and individual interest, where the large amount of sensitive data is in the hand of government authorities as well as private entities.

Aadhaar scheme is one of the initiative taken by government with the advancement of information technology. It is one of the largest scheme to establish the identity of an individual by gathering the biometric and demographic data. The earlier scheme was started in 2009, without any legislative protection later in 2016, Aadhaar Act, 2016 was passed to give legal sanction to the scheme. Scheme is aimed at the delivery of services to targeted beneficiary of government services and benefits. The issue privacy of data arose with the passing of law. Data collected under the Aadhaar project is sensitive in nature should be used with caution but the government is making it mandatory for the entitlement of basic which may hamper the privacy of individual if data goes in wrong hand in this process. The Aadhaar Act, 2016 has no strong mechanism for protection of information. There are loopholes in the Act. There is urgent need to revisit the Act in the present context, to ensure the fundamental right to privacy.

The suggestion in reference to the right to privacy

1. Now the right to privacy stands as the fundamental right in India which raised the many problematic issues. So all the existing laws should be amended accordingly to right to privacy if there is a chance that right to privacy will be a hurdle in smooth running of laws i.e. Provision of search and seizure in the code of criminal procedure, 1973.
2. A national privacy policy should be formed in the consonance of the civil right guaranteed under the constitution and other prevailing laws. It should also follow the set of the norm of Organization for Economic Cooperation and Development guidelines.
3. There is no need for separate legislation as right to privacy bill (pending in parliament). Instead of it part III of the constitution shall be amended accordingly to insert a new article after Article 21. It may be read as “citizen of India has the right to privacy in their personal life, correspondence, at home provide that this right is subject to Article 19(2) of the constitution”. Right to privacy should not be confer on the non-

citizen under article 21. It may hamper the administration of security over territory.

4. In the definition clause of the constitution of India term, “privacy” should be defined. What does it mean and what is ambit of privacy?
5. Everyone has the right to preserve own body-related information. Information regarding the health of individual should be kept secret by the law. There is need of law like “Health Insurance Portability and Accountability Act, 1996” (HIPAA) in the United States, which ensure the privacy, fraud protection in health-related issues.[2]

The suggestion in reference to Aadhaar Act, 2016

The Act is formulated to deliver the services to actually targeted beneficiaries. There is privacy concern over the data gathered for the identification of an individual, as it contains the biometric and demographic data. The consideration of privacy appears to minimal in the Act.[3] Following are the suggestions:

1. The authority (UIDAI) should be given less discretion in framing regulations. There should be a certain fixed norm to apply such discretion.
2. There is a need of a strict privacy policy, which seems to be lacking. The court should prepare strict privacy policy.
3. The provision concerning the protection of information should be strengthened.
4. Punishment under Section 37 and Section 38 of the Act should be severe as it is minimal in amount.
5. Offences relating unauthorized access to data and breach of confidentiality in this reference this under the Act should be made cognizable and non-bailable to ensure the privacy of data.

---

[2] Data Protection Laws In India And Privacy Rights In India, *available at* : http://ptlb.in/clpic/wp-content/uploads/2014/01/Data-Protection-Laws-In-India-And-Privacy-Rights-In-India.pdf (visited on 25 march 2018)

[3] Renuka Sane and Vrinda Bhandari, “Privacy concerns in the Aadhaar Act, 2016”, *available at* : https://www.medianama.com/2016/07/223-privacy-concerns-aadhaar-act-2016/ (visited on 24 april 2018)

BIBLOGRAPGY

BOOKS

1. Neethling, J. and Potgieter, J.M. "*Neethling's law of personality"* 36(Butterworths Durban:.1996)
2. McGarry, K. (1993). *The Changing Context of Information. An Introductory Analysis,* 178 (Library Association Publishing ,London 2nd edn.).
3. John Stuart Mill, *Of Liberty , Utilitarianism And Other Essay*, (oxford university press, oxford, 2005).
4. Lakhwinder singh, *Right To Privacy And Freedom Of Media, 5 (*Satyam Law Publisher , edn. 1 2016
5. Thomas Cooley, *Treatise On The Law Of Torts,(* 2nd edn. 1888).
6. Richard H. Rovere and Gene *Brown, Loyalty and Security in a Democratic State*,354 (New York: Ayer Company Publishers, 1977).
7. DionysiosPolitis, *Socioeconomic And Legal Implications Of Electronic Intrusion* , 131(London: IGI Global, 2009) .
8. Ian Brownlie CBE, QC and Guy s. Goodwin (eds.), *Basic Documents on Human Right*,(Oxford university press Indian edition, 2007).
9. Walter Kalin and Jorg Kunzli, *The Law of International Human Right Protection*, (Oxford university press, 2011).
10. Ian j. Lloyd, *Information Technology Law* (Oxford, edition 7, 2014).
11. Diane Rouland and Uta Kohl, *Information Technology Law,* (Routledge, edn. 4th 2012
12. Nina Godbole, *Information System Security, Security Management, Metrics Frameworks and Best Practices* (Wiley, 2015).
13. Karnika Seth, *Computer Internet and New Technology Laws,* (Lexis Nexis, 2013).
14. R. K. Chaubey, *An Introduction To Cybercrime and Cyber Law* (Kamal Law House, Calcutta, 2nd edn., 2012).

15. S.k. Bansal, *Cyber Crime*,(A P H Publishing corporation,new delhi, 2013).
16. Leslie P. Francis and John G. Francis, *privacy what everyone needs to know* 2,(oxford university press , New Delhi 2017)
17. R. K. Chaubey, "*An Introduction To Cybercrime And Cyber Law"*, 929 (Kamal Law House, Calcutta, 2nd edn., 2012).
18. Dionysios Politis, Socioeconomic and Legal Implications of Electronic Intrusion, 131 (London: IGI Global, 2009).

ARTICLES

1. Warren & Brandeis. "Right to Privacy" 4 *HLR* 193. (1890).
2. Ali Ahmed, David Booth, *The Digital Privacy Laws and Practices in the Jersey Island*, *PCS* 98 (2016) 163 – 168.
3. Gargi Rajvanshi and Myank Singhal, "Data Privacy Law And Growth Of E-Commerce: An Indian Prospective" BLR 1 (2016
4. Clare Sullivan, Digital identity," Privacy and The Right to Identity in the United States Of America", *CLSR* 29 (2013)348-358.
5. Rolf H. Weber, "The Digital Future E-A Challenge For Privacy?", *CLSR* 31 (2015) 234-242
6. Shirin Elahi, "Privacy and consent in the digital era", *Information Security Technical Report* 14 (2009) 113-118.
7. Amba Uttara Kak and Swati Malik, "Privacy and The National Identification Authority Of India Bill: Leaving Much To The Imagination", 3(4) *NUJSLR* 485(2010)
8. Stephanie J. Bird," Security and Privacy: Why Privacy Matters" *Sci Eng Ethics* (2013) 19:669–671
9. Kalyani menon sen," Aadhaar: Wrong Number, Or Big Brother Calling?", 11(2) *SLR* 85 (2015.
10. Guido Noto La Diega, "The Internet of Citizens: A Lawyer's View On Some Technological Developments In The United Kingdom And India", 12 *IJLR & Tech.* 53 (2016).
11. Pramod K Nayar, "'I Sing the Body Biometric' Surveillance and Biological Citizenship", *EPW,* Vol. 47, No. 32 (AUGUST 11, 2012), pp. 17, 19-

12. Collier, G. (1994). Information privacy. Just how private are the details of individuals in a company's database? *IMCS* 3 (1): 41-45
13. Ware, W.H "The New Faces Of Privacy", *The Information Society*, 9 (3): 205 (1993).
14. Michel c james. " A Comparative Analysis Of The Right To Privacy In The United States, Canada , Europe", *Connecticut journal of international law* vol. 29, issue 2 at page 261 (spring 2014
15. William L. Prosser ," privacy *", 48 CLR*. 383 , 389,(1960).
16. Michael J. Sandel," Moral Argument and Liberal Toleration: Abortion and Homosexuality", 77 *CLR* 521, 527-28 (1989
17. H.J. Hermann, "Pulling the Fig Leaf off The Right Of Privacy: Sex And The Constitution", 54 *DLR* 909, 928-930 (2005).
18. J. J. Britz, Technology As A Threat To Privacy: Ethical Challenges to the Information Profession *available at:* http://web.simmons.edu/~chen/nit/NIT%2 796/96-025-Britz.html (visited on January 24, 2018).
19. A. Allen& M Rotenberg, *Privacy Law and Society* (West Academic, New York 2016), *available at:* http://www.maria-online.com/electronics/Article.php?lg =en&q=Right_to _privacy (visited on 15 November 2017).
20. Sam Makkan, Privacy, Parliament & The Judiciary *available at*: http://www.actnow.or g.uk/media/articles/Privacy_Parliament_and_ the_Judiciary.pdf (visited on 8 April 2018).
21. Venkatesh Nayak, Understanding the Right to Privacy, History, Jurisprudence and Implications for India's RTI Regime *available at:* http://cic.gov.in/sites /default/files/2012 /R2Privacy-Venkatesh.pdf (visited on 10 may 2018).
22. Gautam Bhatia, The Supreme Court's Right to Privacy Judgement, available at: http://www.livelaw.in/supreme-courts-right-privacy-judgment-foundations/ (visited on 5 April 2018).
23. Gordon Neal Diem, Locke, Hobbes and the Free Nation available at: http://www.freenati on. org/a/f53d2.html (visited on 25 April 2018).

24. Hem Raj Singh, AADHAAR Act is it Fraud on the Constitution?, available at: http://www.web.lawyersupdate.co.in/cover-story/aadhaar-act-is-it-fraud-on-the-constitution/ (visited on 10 April 2018).

WEBSITE

1. http://www.jstor.org
2. http://link.springer.com
3. http://delnet.nic.in
4. http://home.heinonline.org
5. http://www.manupatra.com
6. http://login.westlawindia.com

STATUE

1. Constitution of India
2. Information Technology Act, 2000
3. Aadhaar Act, 2016

APPENDIX-A

THE AADHAAR (TARGETED DELIVERY OF FINANCIAL AND OTHER SUBSIDIES, BENEFITS AND SERVICES) ACT, 2016

[25th *March*, 2016.]

An Act to provide for, as a good governance, efficient, transparent, and targeted delivery of subsidies, benefits and services, the expenditure for which is incurred from the Consolidated Fund of India, to individuals residing in India through assigning of unique identity numbers to such individuals and for matters connected therewith or incidental thereto.

BE it enacted by Parliament in the Sixty-seventh Year of the Republic of India as follows:—

CHAPTER 1

PRELIMINARY

1. Short title, extent and commen-cement. (*1*) This Act may be called the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

(*2*) It shall extend to the whole of India except the State of Jammu and Kashmir and save as otherwise provided in this Act, it shall also apply to any offence or contravention thereunder committed outside India by any person.

(*3*) It shall come into force on such date as the Central Government may, by notification in the Official Gazette, appoint; and different dates may, be appointed for different provisions of this Act and any reference in any such provision to the commencement of this Act shall be construed as a reference to the commencement of that provision.

2. Definitions In this Act, unless the context otherwise requires,—

a) "Aadhaar Number" means an identification number issued to an individual under sub-section (*3*) of section 3;

b) "Aadhaar Number Holder" means an individual who has been issued an Aadhaar number under this Act;

c) "Authentication" means the process by which the Aadhaar number along with demographic information or biometric information of an individual is submitted

to the Central Identities Data Repository for its verification and such Repository verifies the correctness, or the lack thereof, on the basis of information available with it;

d) "Authentication Record" means the record of the time of authentication and identity of the requesting entity and the response provided by the Authority thereto;

e) "Authority" means the Unique Identification Authority of India established under sub-section (*1*) of section 11;

f) "Benefit" means any advantage, gift, reward, relief, or payment, in cash or kind, provided to an individual or a group of individuals and includes such other benefits as may be notified by the Central Government;

g) "Biometric Information" means photograph, finger print, Iris scan, or such other biological attributes of an individual as may be specified by regulations;

h) "Central Identities Data Repository" means a centralised database in one or more locations containing all Aadhaar numbers issued to Aadhaar number holders along with the corresponding demographic information and biometric information of such individuals and other information related thereto;

i) "Chairperson" means the Chairperson of the Authority appointed under section 12;

j) "Core Biometric Information" means finger print, Iris scan, or such other biological attribute of an individual as may be specified by regulations;

k) "Demographic Information" includes information relating to the name, date of birth, address and other relevant information of an individual, as may be specified by regulations for the purpose of issuing an Aadhaar number, but shall not include race, religion, caste, tribe, ethnicity, language, records of entitlement, income or medical history;

l) "Enrolling Agency" means an agency appointed by the Authority or a Registrar, as the case may be, for collecting demographic and biometric information of individuals under this Act;

m) "Enrolment" means the process, as may be specified by regulations, to collect demographic and biometric information from individuals by the enrolling

agencies for the purpose of issuing Aadhaar numbers to such individuals under this Act;

n) "Identity Information" in respect of an individual, includes his Aadhaar number, his biometric information and his demographic information;

o) "Member" includes the Chairperson and Member of the Authority appointed under section 12;

p) "Notification" means a notification published in the Official Gazette and the expression "notified" with its cognate meanings and grammatical variations shall be construed accordingly;

q) "Prescribed" means prescribed by rules made by the Central Government under this Act;

r) "Records of entitlement" means records of benefits, subsidies or services provided to, or availed by, any individual under any programme;

s) "Registrar" means any entity authorised or recognised by the Authority for the purpose of enrolling individuals under this Act;

t) "Regulations" means the regulations made by the Authority under this Act;

u) "Requesting entity" means an agency or person that submits the Aadhaar number, and demographic information or biometric information, of an individual to the Central Identities Data Repository for authentication;

v) "Resident" means an individual who has resided in India for a period or periods amounting in all to one hundred and eighty-two days or more in the twelve months immediately preceding the date of application for enrolment;

w) "Service" means any provision, facility, utility or any other assistance provided in any form to an individual or a group of individuals and includes such other services as may be notified by the Central Government;

x) "Subsidy" means any form of aid, support, grant, subvention, or appropriation, in cash or kind, to an individual or a group of individuals and includes such other subsidies as may be notified by the Central Government.

CHAPTER II
ENROLMENT

3. Aadhaar number (*1*) Every resident shall be entitled to obtain an Aadhaar number by submitting his demographic information and biometric information by undergoing the process of enrolment:

Provided that the Central Government may, from time to time, notify such other category of individuals who may be entitled to obtain an Aadhaar number.

(*2*) The enrolling agency shall, at the time of enrolment, inform the individual undergoing enrolment of the following details in such manner as may be specified by regulations, namely:—

a. the manner in which the information shall be used;

b. the nature of recipients with whom the information is intended to be shared during authentication; and

c. the existence of a right to access information, the procedure for making requests for such access, and details of the person or department in-charge to whom such requests can be made.

(*3*) On receipt of the demographic information and biometric information under sub-section (*1*), the Authority shall, after verifying the information, in such manner as may be specified by regulations, issue an Aadhaar number to such individual.

4. Properties of Aadhaar number (*1*) An Aadhaar number, issued to an individual shall not be re-assigned to any other individual.

(2) An Aadhaar number shall be a random number and bear no relation to the attributes or identity of the Aadhaar number holder.(*3*) An Aadhaar number, in physical or electronic form subject to authentication and other conditions, as may be specified by regulations, may be accepted as proof of identity of the Aadhaar number holder for any purpose.

***Explanation:* —** for the purposes of this sub-section, the expression "electronic form" shall have the same meaning as assigned to it in clause (*r*) of sub-section (*1*) of section 2 of the Information Technology Act, 2000.

5. Special measures for issuance of Aadhaar number to certain category of persons The Authority shall take special measures to issue Aadhaar number to women, children, senior citizens, persons with disability, unskilled and unorganised workers, nomadic tribes or to such other persons who do not have any permanent dwelling house and such other categories of individuals as may be specified by regulations.

6. Update of certain information The Authority may require Aadhaar number holders to update their demographic information and biometric information, from time to time, in such manner as may be specified by regulations, so as to ensure continued accuracy of their information in the Central Identities Data Repository.

CHAPTER III

AUTHENTICATION

Proof of Aadhaar number necessary for receipt of certain subsidies, benefits and services, etc.7. The Central Government or, as the case may be, the State Government may, for the purpose of establishing identity of an individual as a condition for receipt of a subsidy, benefit or service for which the expenditure is incurred from, or the receipt therefrom forms part of, the Consolidated Fund of India, require that such individual undergo authentication, or furnish proof of possession of Aadhaar number or in the case of an individual to whom no Aadhaar number has been assigned, such individual makes an application for enrolment:

7. Proof of Aadhaar number necessary for receipt of certain subsidies, benefits and services, etc:- The Central Government or, as the case may be, the State Government may, for the purpose of establishing identity of an individual as a condition for receipt of a subsidy, benefit or service for which the expenditure is incurred from, or the receipt therefrom forms part of, the Consolidated Fund of India, require that such individual undergo authentication, or furnish proof of possession of Aadhaar number or in the case of an individual to whom no Aadhaar number has been assigned, such individual makes an application for enrolment:

Provided that if an Aadhaar number is not assigned to an individual, the individual shall be offered alternate and viable means of identification for delivery of the subsidy, benefit or service.

8. Authentication of Aadhaar number. (*1*) The Authority shall perform authentication of the Aadhaar number of an Aadhaar number holder submitted by any requesting entity, in relation to his biometric information or demographic information, subject to such conditions and on payment of such fees and in such manner as may be specified by regulations.

(*2*) A requesting entity shall—

(*a*) Unless otherwise provided in this Act, obtain the consent of an individual before collecting his identity information for the purposes of authentication in such manner as may be specified by regulations; and

(*b*) Ensure that the identity information of an individual is only used for submission to the Central Identities Data Repository for authentication.

(*3*) A requesting entity shall inform, in such manner as may be specified by regulations, the individual submitting his identity information for authentication, the following details with respect to authentication, namely:—

(*a*) The nature of information that may be shared upon authentication;

(*b*) The uses to which the information received during authentication may be put by the requesting entity; and

(*c*) Alternatives to submission of identity information to the requesting entity.

(*4*) The Authority shall respond to an authentication query with a positive, negative or any other appropriate response sharing such identity information excluding any core biometric information.

9. Aadhaar number not evidence of citizenship or domicile, etc. The Aadhaar number or the authentication thereof shall not, by itself, confer any right of, or be proof of, citizenship or domicile in respect of an Aadhaar number holder.

10. Central Identities Data Repository. The Authority may engage one or more entities to establish and maintain the Central Identities Data Repository and to perform any other functions as may be specified by regulations.

CHAPTER IV
UNIQUE IDENTIFICATION AUTHORITY OF INDIA

11. Establishment of Authority:- (*1*) The Central Government shall, by notification, establish an Authority to be known as the Unique Identification Authority of India to be responsible for the processes of enrolment and authentication and perform such other functions assigned to it under this Act.

(*2*) The Authority shall be a body corporate by the name aforesaid, having perpetual succession and a common seal, with power, subject to the provisions of

this Act, to acquire, hold and dispose of property, both movable and immovable, and to contract, and shall, by the said name, sue or be sued.

(*3*) The head office of the Authority shall be in New Delhi.

(*4*) The Authority may, with the prior approval of the Central Government, establish its offices at other places in India.

12. Composition of Authority. The Authority shall consist of a Chairperson, appointed on part-time or full- time basis, two part-time Members, and the chief executive officer who shall be Member-Secretary of the Authority, to be appointed by the Central Government.

13. Qualifications for appointment of Chairperson and Members of Authority. The Chairperson and Members of the Authority shall be persons of ability and integrity having experience and knowledge of at least ten years in matters relating to technology, governance, law, development, economics, finance, management, public affairs or administration.

14. Term of office and Other conditions of service of Chairperson and Members (*1*) The Chairperson and the Members appointed under this Act shall hold office for a term of three years from the date on which they assume office and shall be eligible for re-appointment:

Provided that no person shall hold office as the Chairperson or Member after he has attained the age of sixty-five years.

(*2*) The Chairperson and every Member shall, before entering office, make and subscribe to, an oath of office and of secrecy, in such form and in such manner and before such Authority as may be prescribed.

(*3*) Notwithstanding anything contained in sub-section (*1*), the Chairperson or Member may—

(*a*) Relinquish his office, by giving in writing to the Central Government, a notice of not less than thirty days; or

(*b*) Be removed from his office in accordance with the provisions of section 15.

(*4*) The salaries and allowances payable to, and the other terms and conditions of service of, the Chairperson and allowances or remuneration payable to part-time Members shall be such as may be prescribed.

15. Removal of Chairperson and Members. (*1*) The Central Government may remove from office, the Chairperson, or a Member, who—

(*a*) Is, or at any time has been adjudged as insolvent;

(*b*) Has become physically or mentally incapable of acting as the Chairperson or, as the case may be, a Member;

(*c*) Has been convicted of an offence which, in the opinion of the Central Government, involves moral turpitude;

(*d*) Has acquired such financial or other interest as is likely to affect prejudicially his functions as the Chairperson or, as the case may be, a Member; or

(*e*) Has, in the opinion of the Central Government, so abused his position as to render his continuance in office detrimental to the public interest.

(*2*) The Chairperson or a Member shall not be removed under clause (*b*), clause (*d*) or clause (*e*) of sub-section (*1*) unless he has been given a reasonable opportunity of being heard.

16. Restrictions on Chairperson or Members on employment after cessation of office. The Chairperson or a Member on ceasing to hold office for any reason, shall not, without previous approval of the Central Government,—

(*a*) Accept any employment in, or be connected with the management of any organisation, company or any other entity which has been associated with any work done or contracted out by the Authority, whether directly or indirectly, during his tenure as Chairperson or Member, as the case may be, for a period of three years from the date on which he ceases to hold office:

Provided that nothing contained in this clause shall apply to any employment under the Central Government or a State Government or local authority or in any statutory authority or any corporation established by or under any Central, State or provincial Act or a Government Company, as defined in clause (*45*) of section 2 of the Companies Act, 2013;

(*b*) Act, for or on behalf of any person or organisation in connection with any specific proceeding or transaction or negotiation or a case to which the Authority is a party and with respect to which the Chairperson or such Member had, before cessation of office, acted for or provided advice to, the Authority;

(*c*) Give advice to any person using information which was obtained in his capacity as the Chairperson or a Member and being unavailable to or not being able to be made available to the public; or

(*d*) Enter, for a period of three years from his last day in office, into a contract of service with, accept an appointment to a board of directors of, or accept an offer of employment with, an entity with which he had direct and significant official dealings during his term of office.

17. Functions of Chairperson. The Chairperson shall preside over the meetings of the Authority, and without prejudice to any provision of this Act, exercise and discharge such other powers and functions of the Authority as may be prescribed.

18. Chief executive officer. (*1*) There shall be a chief executive officer of the Authority, not below the rank of Additional Secretary to the Government of India, to be appointed by the Central Government. (*2*) The chief executive officer shall be the legal representative of the Authority and shall be responsible for—

a. The day-to-day administration of the Authority;

b. Implementing the work programmes and decisions adopted by the Authority;

c. Drawing up of proposal for the Authority's decisions and work programmes;

d. The preparation of the statement of revenue and expenditure and the execution of the budget of the Authority; and

e. Performing such other functions, or exercising such other powers, as may be specified by regulations.

(*3*) Every year, the chief executive officer shall submit to the Authority for approval—

(a) A general report covering all the activities of the Authority in the previous year;

(b) Programmes of work;

(c) The annual accounts for the previous year; and

(d) The budget for the coming year.

(*4*) The chief executive officer shall have administrative control over the officers and other employees of the Authority.

19. Meetings of Authority. (*1*) The Authority shall meet at such times and places and shall observe such rules of procedure in regard to the transaction of business at its meetings, including quorum at such meetings, as may be specified by regulations.

(*2*) The Chairperson, or, if for any reason, he is unable to attend a meeting of the Authority, the senior most Member shall preside over the meetings of the Authority.

(*3*) All questions which come up before any meeting of the Authority shall be decided by a majority of votes by the Members present and voting and in the event of an equality of votes, the Chairperson or in his absence the presiding Member shall have a casting vote.

(*4*) All decisions of the Authority shall be signed by the Chairperson or any other Member or the Member-Secretary authorised by the Authority in this behalf.

(*5*) If any Member, who is a director of a company and who as such director, has any direct or indirect pecuniary interest in any manner coming up for consideration at a meeting of the Authority, he shall, as soon as possible after relevant circumstances have come to his knowledge, disclose the nature of his interest at such meeting and such disclosure shall be recorded in the proceedings of the Authority, and the Member shall not take part in any deliberation or decision of the Authority with respect to that matter.

20. Vacancies, etc., not to invalidate proceedings of Authority. No act or proceeding of the Authority shall be invalid merely by reason of— (*a*) any vacancy in, or any defect in the constitution of, the Authority;

(*b*) Any defect in the appointment of a person as Chairperson or Member of the Authority; or

(*c*) Any irregularity in the procedure of the Authority not affecting the merits of the case.

21. Officers and other employees of Authority (*1*) The Authority may, with the approval of the Central Government, determine the number, nature and categories of other officers and employees required by the Authority in the discharge of its functions.

(*2*) The salaries and allowances payable to, and the other terms and conditions of service of, the chief executive officer and other officers and other employees of the Authority shall be such as may be specified by regulations with the approval of the Central Government.

22. Transfer of assets, liabilities of Authority On and from the establishment of the Authority— (*a*) all the assets and liabilities of the Unique Identification Authority of India, established *vide* notification of the Government of India in the Planning Commission number A-43011/02/2009-Admin. I, dated the 28th January, 2009, shall stand transferred to, and vested in, the Authority.

***Explanation*.—**The assets of such Unique Identification Authority of India shall be deemed to include all rights and powers, and all properties, whether movable or immovable, including, in particular, cash balances, deposits and all other interests and rights in, or arising out of, such properties as may be in the possession of such Unique Identification Authority of India and all books of account and other documents relating to the same; and liabilities shall be deemed to include all debts, liabilities and obligations of whatever kind;

(*b*) Without prejudice to the provisions of clause (*a*), all data and information collected during enrolment, all details of authentication performed, debts, obligations and liabilities incurred, all contracts entered into and all matters and things engaged to be done by, with or for such Unique Identification Authority of India immediately before that day, for or in connection with the purpose of the said Unique Identification Authority of India, shall be deemed to have been incurred, entered into or engaged to be done by, with or for, the Authority;

(*c*) All sums of money due to the said Unique Identification Authority of India immediately before that day shall be deemed to be due to the Authority; and

(*d*) All suits and other legal proceedings instituted or which could have been instituted by or against such Unique Identification Authority of India immediately before that day may be continued or may be instituted by or against the Authority.

23. Powers and functions of Authority (*1*) The Authority shall develop the policy, procedure and systems for issuing Aadhaar numbers to individuals and perform authentication thereof under this Act.

(*2*) Without prejudice to sub-section (*1*), the powers and functions of the Authority, *inter alia,* include—

(*a*) Specifying, by regulations, demographic information and biometric information required for enrolment and the processes for collection and verification thereof;

(*b*) Collecting demographic information and biometric information from any individual seeking an Aadhaar number in such manner as may be specified by regulations;

(*c*) Appointing of one or more entities to operate the Central Identities Data Repository;

(*d*) Generating and assigning Aadhaar numbers to individuals; (*e*) performing authentication of Aadhaar numbers;

(*f*) Maintaining and updating the information of individuals in the Central Identities Data Repository in such manner as may be specified by regulations;

(*g*) Omitting and deactivating of an Aadhaar number and information relating thereto in such manner as may be specified by regulations;

(*h*) Specifying the manner of use of Aadhaar numbers for the purposes of providing or availing of various subsidies, benefits, services and other purposes for which Aadhaar numbers may be used;

(*i*) Specifying, by regulations, the terms and conditions for appointment of Registrars, enrolling agencies and service providers and revocation of appointments thereof;

(*j*) Establishing, operating and maintaining of the Central Identities Data Repository;

(*k*) Sharing, in such manner as may be specified by regulations, the information of Aadhaar number holders, subject to the provisions of this Act;

(*l*) Calling for information and records, conducting inspections, inquiries and audit of the operations for the purposes of this Act of the Central Identities Data Repository, Registrars, enrolling agencies and other agencies appointed under this Act;

(*m*) Specifying, by regulations, various processes relating to data management, security protocols and other technology safeguards under this Act;

(*n*) Specifying, by regulations, the conditions and procedures for issuance of new Aadhaar number to existing Aadhaar number holder;

(*o*) levying and collecting the fees or authorising the Registrars, enrolling agencies or other service providers to collect such fees for the services provided by them under this Act in such manner as may be specified by regulations;

(*p*) Appointing such committees as may be necessary to assist the Authority in discharge of its functions for the purposes of this Act;

(*q*) Promoting research and development for advancement in biometrics and related areas, including usage of Aadhaar numbers through appropriate mechanisms;

(*r*) Evolving of, and specifying, by regulations, policies and practices for Registrars, enrolling agencies and other service providers;

(*s*) Setting up facilitation centres and grievance redressal mechanism for redressal of grievances of individuals, Registrars, enrolling agencies and other service providers;

(*t*) Such other powers and functions as may be prescribed.

(*3*) The Authority may,—

(*a*) enter into Memorandum of Understanding or agreement, as the case may be, with the Central Government or State Governments or Union territories or other agencies for the purpose of performing any of the functions in relation to collecting, storing, securing or processing of information or delivery of Aadhaar numbers to individuals or performing authentication;

(*b*) By notification, appoint such number of Registrars, engage and authorise such agencies to collect, store, secure, process information or do authentication or perform such other functions in relation thereto, as may be necessary for the purposes of this Act.

(*4*) The Authority may engage such consultants, advisors and other persons as may be required for efficient discharge of its functions under this Act on such allowances or remuneration and terms and conditions as may be specified by contract.

CHAPTER V

GRANTS, ACCOUNTS AND AUDIT AND ANNUAL REPORT

24. Grants by Central Government:- The Central Government may, after due appropriation made by Parliament by law in this behalf, make to the Authority, grants of such sums of money as the Central Government may think fit for being utilised for the purposes of this Act.

25. Other fees and revenues. The fees or revenue collected by the Authority shall be credited to the Consolidated Fund of India.

26. Accounts and audit. (*1*) The Authority shall maintain proper accounts and other relevant records and prepare an annual statement of accounts in such form as may be prescribed by the Central Government in consultation with the Comptroller and Auditor-General of India.

(*2*) The accounts of the Authority shall be audited annually by the Comptroller and Auditor-General of India at such intervals as may be specified by him and any expenditure incurred in connection with such audit shall be payable by the Authority to the Comptroller and Auditor-General.

(*3*) The Comptroller and Auditor-General of India and any person appointed by him in connection with the audit the accounts of the Authority under this Act shall have the same rights and privileges and authority in connection with such audit as the Comptroller and Auditor-General generally has in connection with the audit of Government accounts, and in particular, shall have the right to demand production of books, accounts, connected vouchers and other documents and papers, and to inspect any of the offices of the Authority.

(*4*) The accounts of the Authority, as certified by the Comptroller and Auditor-General of India or any other person appointed by him in this behalf, together with the audit report thereon shall be forwarded annually to the Central Government by the Authority and the Central Government shall cause the audit report to be laid, as soon as may be after it is received, before each House of Parliament.

27. Returns and annual report, etc. (*1*) The Authority shall furnish to the Central Government at such time and in such form and manner as may be prescribed or as the Central Government may direct, such returns and statements and particulars in regard to any matter under the jurisdiction of the Authority, as the Central Government may from time to time require.

(*2*) The Authority shall prepare, once in every year, and in such form and manner and at such time as may be prescribed, an annual report giving—

(*a*) A description of all the activities of the Authority for the previous years;

(*b*) The annual accounts for the previous year; and

(*c*) The programmes of work for coming year.

(*3*) A copy of the report received under sub-section (*2*) shall be laid by the Central Government, as soon as may be after it is received, before each House of Parliament.

CHAPTER VI
PROTECTION OF INFORMATION

28. Security and confidentiality of information (*1*) The Authority shall ensure the security of identity information and authentication records of individuals.

(*2*) Subject to the provisions of this Act, the Authority shall ensure confidentiality of identity information and authentication records of individuals.

(*3*) The Authority shall take all necessary measures to ensure that the information in the possession or control of the Authority, including information stored in the Central Identities Data Repository, is secured and protected against access, use or disclosure not permitted under this Act or regulations made thereunder, and against accidental or intentional destruction, loss or damage.

(*4*) Without prejudice to sub-sections (*1*) and (*2*), the Authority shall—

(*a*) Adopt and implement appropriate technical and organisational security measures;

(*b*) Ensure that the agencies, consultants, advisors or other persons appointed or engaged for performing any function of the Authority under this Act, have in place appropriate technical and organisational security measures for the information; and

(*c*) Ensure that the agreements or arrangements entered into with such agencies, consultants, advisors or other persons, impose obligations equivalent to those imposed on the Authority under this Act, and require such agencies, consultants, advisors and other persons to act only on instructions from the Authority.

(*5*) Notwithstanding anything contained in any other law for the time being in force, and save as otherwise provided in this Act, the Authority or any of its officers or other employees or any agency that maintains the Central Identities Data

Repository shall not, whether during his service or thereafter, reveal any information stored in the Central Identities Data Repository or authentication record to anyone:

Provided that an Aadhaar number holder may request the Authority to provide access to his identity information excluding his core biometric information in such manner as may be specified by regulations.

29. Restriction on sharing information (*1*) No core biometric information, collected or created under this Act, shall be— (*a*) shared with anyone for any reason whatsoever; or

(*b*) used for any purpose other than generation of Aadhaar numbers and authentication under this Act.

(*2*) The identity information, other than core biometric information, collected or created under this Act may be shared only in accordance with the provisions of this Act and in such manner as may be specified by regulations.

(*3*) No identity information available with a requesting entity shall be—

(*a*) Used for any purpose, other than that specified to the individual at the time of submitting any identity information for authentication; or

(*b*) Disclosed further, except with the prior consent of the individual to whom such information relates.

(*4*) No Aadhaar number or core biometric information collected or created under this Act in respect of an Aadhaar number holder shall be published, displayed or posted publicly, except for the purposes as may be specified by regulations.

30. Biometric information deemed to be sensitive personal information. The biometric information collected and stored in electronic form, in accordance with this Act and regulations made thereunder, shall be deemed to be "electronic record" and "sensitive personal data or information", and the provisions contained in the Information Technology Act, 2000 and the rules made thereunder shall apply to such information, in addition to, and to the extent not in derogation of the provisions of this Act.

Explanation.— For the purposes of this section, the expressions—

(*a*) "Electronic form" shall have the same meaning as assigned to it in clause (*r*) of sub-section (*1*) of section 2 of the Information Technology Act, 2000;

(*b*) “Electronic record” shall have the same meaning as assigned to it in clause (*t*) of sub-section (*1*) of section 2 of the Information Technology Act, 2000;

(*c*) “Sensitive personal data or information” shall have the same meaning as assigned to it in clause (*iii*) of the *Explanation* to section 43A of the Information Technology Act, 2000.

31. Alteration of demographic information or biometric information. (*1*) In case any demographic information of an Aadhaar number holder is found incorrect or changes subsequently, the Aadhaar number holder shall request the Authority to alter such demographic information in his record in the Central Identities Data Repository in such manner as may be specified by regulations.

(*2*) In case any biometric information of Aadhaar number holder is lost or changes subsequently for any reason, the Aadhaar number holder shall request the Authority to make necessary alteration in his record in the Central Identities Data Repository in such manner as may be specified by regulations.

(*3*) On receipt of any request under sub-section (*1*) or sub-section (*2*), the Authority may, if it is satisfied, make such alteration as may be required in the record relating to such Aadhaar number holder and intimate such alteration to the concerned Aadhaar number holder.

(*4*) No identity information in the Central Identities Data Repository shall be altered except in the manner provided in this Act or regulations made in this behalf.

32. Access to own information and records of requests for authentication. (*1*) The Authority shall maintain authentication records in such manner and for such period as may be specified by regulations.

(*2*) Every Aadhaar number holder shall be entitled to obtain his authentication record in such manner as may be specified by regulations.

(*3*) The Authority shall not, either by itself or through any entity under its control, collect, keep or maintain any information about the purpose of authentication.

33. Disclosure of information in certain cases. (*1*) Nothing contained in sub-section (*2*) or sub-section (*5*) of section 28 or sub-section (*2*) of section 29 shall apply in respect of any disclosure of information, including identity information or authentication records, made pursuant to an order of a court not inferior to that of a District Judge:

Provided that no order by the court under this sub-section shall be made without giving an opportunity of hearing to the Authority.

(*2*) Nothing contained in sub-section (*2*) or sub-section (*5*) of section 28 and clause (*b*) of sub-section (*1*), sub-section (*2*) or sub-section (*3*) of section 29 shall apply in respect of any disclosure of information, including identity information or authentication records, made in the interest of national security in pursuance of a direction of an officer not below the rank of Joint Secretary to the Government of India specially authorised in this behalf by an order of the Central Government:

Provided that every direction issued under this sub-section, shall be reviewed by an Oversight Committee consisting of the Cabinet Secretary and the Secretaries to the Government of India in the Department of Legal Affairs and the Department of Electronics and Information Technology, before it takes effect:

Provided further that any direction issued under this sub-section shall be valid for a period of three months from the date of its issue, which may be extended for a further period of three months after the review by the Oversight Committee.

CHAPTER VII
OFFENCES AND PENALTIES

34. Penalty for impersonation at time of enrolment. Whoever impersonates or attempts to impersonate another person, whether dead or alive, real or imaginary, by providing any false demographic information or biometric information, shall be punishable with imprisonment for a term which may extend to three years or with a fine which may extend to ten thousand rupees or with both.

35. Penalty for impersonation of Aadhaar number holder by changing demographic information or biometric information. Whoever, with the intention of causing harm or mischief to an Aadhaar number holder, or with the intention of appropriating the identity of an Aadhaar number holder changes or attempts to change any demographic information or biometric information of an Aadhaar number holder by impersonating or attempting to impersonate another person, dead or alive, real or imaginary, shall be punishable with imprisonment for

a term which may extend to three years and shall also be liable to a fine which may extend to ten thousand rupees.

36. Penalty for impersonation. Whoever, not being authorised to collect identity information under the provisions of this Act, by words, conduct or demeanour pretends that he is authorized to do so, shall be punishable with imprisonment for a term which may extend to three years or with a fine which may extend to ten thousand rupees or, in the case of a company, with a fine which may extend to one lakh rupees or with both.

37. Penalty for disclosing identity information. Whoever, intentionally discloses, transmits, copies or otherwise disseminates any identity information collected in the course of enrolment or authentication to any person not authorized under this Act or regulations made thereunder or in contravention of any agreement or arrangement entered into pursuant to the provisions of this Act, shall be punishable with imprisonment for a term which may extend to three years or with a fine which may extend to ten thousand rupees or, in the case of a company, with a fine which may extend to one lakh rupees or with both.

38. Penalty for unauthorized access to the Central Identities Data Repository. Whoever, not being authorized by the Authority, intentionally,—

(*a*) Accesses or secures access to the Central Identities Data Repository;

(*b*) Downloads, copies or extracts any data from the Central Identities Data Repository or stored in any removable storage medium;

(*c*) Introduces or causes to be introduced any virus or other computer contaminant in the Central Identities Data Repository;

(*d*) Damages or causes to be damaged the data in the Central Identities Data Repository;

(*e*) Disrupts or causes disruption of the access to the Central Identities Data Repository;

(*f*) Denies or causes a denial of access to any person who is authorized to access the Central Identities Data Repository.

(*g*) Reveals any information in contravention of sub-section (*5*) of section 28, or shares, uses or displays information in contravention of section 29 or assists any person in any of the aforementioned acts;

(*h*) Destroys, deletes or alters any information stored in any removable storage media or in the Central Identities Data Repository or diminishes its value or utility or affects it injuriously by any means; or

(*i*) steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used by the Authority with an intention to cause damage, shall be punishable with imprisonment for a term which may extend to three years and shall also be liable to a fine which shall not be less than ten lakh rupees. ***Explanation.—*** For the purposes of this section, the expressions "computer contaminant", "computer virus" and "damage" shall have the meanings respectively 21 of 2000. assigned to them in the *Explanation* to section 43 of the Information Technology Act, 2000, and the expression "computer source code" shall have the meaning assigned to it in the *Explanation* to section 65 of the said Act.

39. Penalty for tampering with data in Central Identities Data Repository. Whoever, not being authorized by the Authority, uses or tampers with the data in the Central Identities Data Repository or in any removable storage medium with the intent of modifying information relating to Aadhaar number holder or discovering any information thereof, shall be punishable with imprisonment for a term which may extend to three years and shall also be liable to a fine which may extend to ten thousand rupees.

40. Penalty for unauthorized use by requesting entity. Whoever, being a requesting entity, uses the identity information of an individual in contravention of sub-section (*3*) of section 8, shall be punishable with imprisonment which may extend to three years or with a fine which may extend to ten thousand rupees or, in the case of a company, with a fine which may extend to one lakh rupees or with both.

41. Penalty for non- compliance with intimation requirements. Whoever, being an enrolling agency or a requesting entity, fails to comply with the requirements of sub-section (*2*) of section 3 or sub-section (*3*) of section 8, shall be punishable with imprisonment which may extend to one year or with a fine which may extend to ten thousand rupees or, in the case of a company, with a fine which may extend to one lakh rupees or with both.

42. General penalty. Whoever commits an offence under this Act or any rules or regulations made there under for which no specific penalty is provided elsewhere than this section, shall be punishable with imprisonment for a term which may extend to one year or with a fine which may extend to twenty-five thousand rupees or, in the case of a company, with a fine which may extend to one lakh rupees, or with both.

43. Offences by companies (*1*) Where an offence under this Act has been committed by a company, every person who at the time the offence was committed was in charge of, and was responsible to, the company for the conduct of the business of the company, as well as the company, shall be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly:

Provided that nothing contained in this sub-section shall render any such person liable to any punishment provided in this Act if he proves that the offence was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence.

(*2*) Notwithstanding anything contained in sub-section (*1*), where any offence under this Act has been committed by a company and it is proved that the offence has been committed with the consent or connivance of, or is attributable to, any neglect on the part of any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly.

Explanation.—for the purposes of this section—

(*a*) "Company" means anybody corporate and includes a firm or other association of individuals; and

(*b*) "Director", in relation to a firm, means a partner in the firm.

44. Act to apply for offence or contravention committed outside India. (*1*) Subject to the provisions of sub-section (*2*), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person, irrespective of his nationality.

(2) for the purpose of sub-section (1), the provision of this Act shall apply to any offence or contravention committed outside India by any persons, if the Act or

conduct constituting the offence or contravention involves any data in the Central Identities Data Repository.

45. Power to investigate offences. Not with standing anything contained in the code of criminal procedure, 1973 (2 of 1974), a police officer not below the rank of inspector of police shall investigate any offence under this Act.

46. Penalties not to interfere with other punishments. No penalty imposed under this Act shall prevent the imposition of any other penalty or punishment under any other law for the time being in force.

47. Cognizance of offences. (*1*) No court shall take cognizance of any offence punishable under this Act, save on a complaint made by the Authority or any officer or person authorized by it.

(*2*) No court inferior to that of a Chief Metropolitan Magistrate or a Chief Judicial Magistrate shall try any offence punishable under this Act.

CHAPTER VIII
MISCELLANEOUS

48. Power of Central Government to supersede Authority. (*1*) If, at any time, the Central Government is of the opinion,—

(*a*) That, on account of circumstances beyond the control of the Authority, it is unable to discharge the functions or perform the duties imposed on it by or under the provisions of this Act; or

(*b*) That the Authority has persistently defaulted in complying with any direction given by the Central Government under this Act or in the discharge of the functions or performance of the duties imposed on it by or under the provisions of this Act and as a result of such default the financial position of the Authority or the administration of the Authority has suffered; or

(*c*) That a public emergency exists, the Central Government may, by notification, supersede the Authority for such period, not exceeding six months, as may be specified in the notification and appoint a person or persons as the President may direct to exercise powers and discharge functions under this Act

Provided that before issuing any such notification, the Central Government shall give a reasonable opportunity to the Authority to make representations against the

proposed supersession and shall consider the representations, if any, of the Authority.

(*2*) Upon the publication of a notification under sub-section (*1*), superseding the Authority,—

(*a*) The Chairperson and other Members shall, as from the date of supersession, vacate their offices as such;

(*b*) All the powers, functions and duties which may, by or under the provisions of this Act, be exercised or discharged by or on behalf of the Authority shall, until the Authority is reconstituted under sub-section (*3*), be exercised and discharged by the person or persons referred to in sub-section (*1*); and

(*c*) All properties owned or controlled by the Authority shall, until the Authority is reconstituted under sub-section (*3*), vest in the Central Government.

(*3*) On or before the expiration of the period of supersession specified in the notification issued under sub-section (*1*), the Central Government shall reconstitute the Authority by a fresh appointment of its Chairperson and other Members and in such case any person who had vacated his office under clause (*a*) of sub-section (*2*) shall not be deemed to be disqualified for reappointment.

(*4*) The Central Government shall cause a copy of the notification issued under sub-section (*1*) and a full report of any action taken under this section and the circumstances leading to such action to be laid before each House of Parliament at the earliest.

49. Members, officers, etc., to be public servants. The Chairperson, Members, officers and other employees of the Authority shall be deemed, while acting or purporting to act in pursuance of any of the provisions of this Act, to be public servants within the meaning of section 21 of the Indian Penal Code.

50. Power of Central Government to issue directions. (*1*) Without prejudice to the foregoing provisions of this Act, the Authority shall, in exercise of its powers or the performance of its functions under this Act be bound by such directions on questions of policy, as the Central Government may give, in writing to it, from time to time:

Provided that the Authority shall, as far as practicable, be given an opportunity to express its views before any direction is given under this sub-section:

Provided further that nothing in this section shall empower the Central Government to issue directions pertaining to technical or administrative matters undertaken by the Authority.

(*2*) The decision of the Central Government, whether a question is one of policy or not, shall be final.

51. Delegation The Authority may, by general or special order in writing, delegate to any Member, officer of the Authority or any other person, subject to such conditions, if any, as may be specified in the order, such of its powers and functions under this Act (except the power under section 54) as it may deem necessary.

52. Protection of action taken in good faith. No suit, prosecution or other legal proceeding shall lie against the Central Government or the Authority or the Chairperson or any Member or any officer, or other employees of the Authority for anything which is in good faith done or intended to be done under this Act or the rule or regulation made thereunder.

53. Power of Central Government to make rules. (*1*) The Central Government may, by notification, make rules to carry out the provisions of this Act.

(*2*) In particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely:—

(*a*) The form and manner in which and the authority before whom the oath of office and of secrecy is to be subscribed by the Chairperson and Members under sub-section (*2*) of section 14;

(*b*) The salary and allowances payable to, and other terms and conditions of service of, the Chairperson and the allowances or remuneration payable to Members of the Authority under sub-section (*4*) of section 14;

(*c*) The other powers and functions of the Chairperson of the Authority under section 17;

(*d*) The other powers and functions of the Authority under clause (*t*) of sub-section (*2*) of section 23;

(*e*) The form of annual statement of accounts to be prepared by Authority under sub-section (*1*) of section 26;

(*f*) The form and the manner in which and the time within which returns and statements and particulars are to be furnished under sub-section (*1*) of section 27;

(*g*) The form and the manner and the time at which the Authority shall furnish annual report under sub-section (*2*) of section 27;

(*h*) Any other matter which is required to be, or may be, prescribed, or in respect of which provision is to be or may be made by rules.

54. Power of Authority to make regulations (*1*) The Authority may, by notification, make regulations consistent with this Act and the rules made thereunder, for carrying out the provisions of this Act.

(*2*) In particular, and without prejudice to the generality of the foregoing power, such regulations may provide for all or any of the following matters, namely:—

(*a*) The biometric information under clause (*g*) and the demographic information under clause (*k*), and the process of collecting demographic information and biometric information from the individuals by enrolling agencies under clause (*m*) of section 2;

(*b*) The manner of verifying the demographic information and biometric information for issue of Aadhaar number under sub-section (*3*) of section 3;

(*c*) The conditions for accepting an Aadhaar number as proof of identity of the Aadhaar number holder under sub-section (*3*) of section 4;

(*d*) The other categories of individuals under section 5 for whom the Authority shall take special measures for allotment of Aadhaar number;

(*e*) The manner of updating biometric information and demographic information under section 6;

(*f*) The procedure for authentication of the Aadhaar number under section 8;

(*g*) The other functions to be performed by the Central Identities Data Repository under section 10;

(*h*) The time and places of meetings of the Authority and the procedure for transaction of business to be followed by it, including the quorum, under sub-section (*1*) of section 19;

(*i*) The salary and allowances payable to, and other terms and conditions of service of, the chief executive officer, officers and other employees of the Authority under sub-section (*2*) of section 21;

(*j*) The demographic information and biometric information under clause (*a*) and the manner of their collection under clause (*b*) of sub-section (*2*) of section 23;

(*k*) The manner of maintaining and updating the information of individuals in the Central Identities Data Repository under clause (*f*) of sub-section (*2*) of section 23.

(*l*) The manner of omitting and deactivating an Aadhaar number and information relating thereto under clause (*g*) of sub-section (*2*) of section 23;

(*m*) The manner of use of Aadhaar numbers for the purposes of providing or availing of various subsidies, benefits, services and other purposes for which Aadhaar numbers may be used under clause (*h*) of sub-section (*2*) of section 23;

(*n*) The terms and conditions for appointment of Registrars, enrolling agencies and other service providers and the revocation of appointments thereof under clause (*i*) of sub-section (*2*) of section 23;

(*o*) The manner of sharing information of Aadhaar number holder under clause (*k*) of sub-section (*2*) of section 23;

(*p*) Various processes relating to data management, security protocol and other technology safeguards under clause (*m*) of sub-section (*2*) of section 23;

(*q*) The procedure for issuance of new Aadhaar number to existing Aadhaar number holder under clause (*n*) of sub-section (*2*) of section 23;

(*r*) Manner of authorising Registrars, enrolling agencies or other service providers to collect such fees for services provided by them under clause (*o*) of sub-section (*2*) of section 23;

(*s*) Policies and practices to be followed by the Registrar, enrolling agencies and other service providers under clause (*r*) of sub-section (*2*) of section 23;

(*t*) The manner of accessing the identity information by the Aadhaar number holder under the proviso to sub-section (*5*) of section 28;

(*u*) The manner of sharing the identity information, other than core biometric information, collected or created under this Act under sub-section (*2*) of section 29;

(*v*) The manner of alteration of demographic information under sub-section (*1*) and biometric information under sub-section (*2*) of section 31;

(*w*) The manner of and the time for maintaining the request for authentication and the response thereon under sub-section (*1*), and the manner of obtaining, by the Aadhaar number holder, the authentication records under sub-section (*2*) of section 32;

(*x*) Any other matter which is required to be, or may be, specified, or in respect of which provision is to be or may be made by regulations.

55. Laying of rules and regulations before Parliament. Every rule and every regulation made under this Act shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the rule or regulation, or both the Houses agree that the rule or regulation should not be made, the rule or regulation shall thereafter have effect only in such modified form or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that rule or regulation.

56. Application of other laws not barred. The provisions of this Act shall be in addition to, and not in derogation of, any other law for the time being in force.

57. Act not to prevent use of Aadhaar number for other purposes under law. Nothing contained in this Act shall prevent the use of Aadhaar number for establishing the identity of an individual for any purpose, whether by the State or any body corporate or person, pursuant to any law, for the time being in force, or any contract to this effect:

Provided that the use of Aadhaar number under this section shall be subject to the procedure and obligations under section 8 and Chapter VI.

58. Power to remove difficulties. (*1*) If any difficulty arises in giving effect to the provisions of this Act, the Central Government may, by order, published in the Official Gazette, make such provisions not inconsistent with the provisions of this Act as may appear to be necessary for removing the difficulty:

Provided that no such order shall be made under this section after the expiry of three years from the commencement of this Act.

(*2*) Every order made under this section shall be laid, as soon as may be after it is made, before each House of Parliament.

59. Savings anything done or any action taken by the Central Government under the Resolution of the Government of India, Planning Commission bearing notification number A-43011/02/2009-Admin. I, dated the 28th January, 2009,

or by the Department of Electronics and Information Technology under the Cabinet Secretariat Notification bearing notification number S.O. 2492(*E*), dated the 12th September, 2015, as the case may be, shall be deemed to have been validly done or taken under this Act.