PERSONAL PRIVACY IN CYBERSPACE

Thesis
Submitted for the award of
Degree of Doctor of Philosophy
Discipline - Law

By
Kamshad

Enrollment No: MUIT0119038067

Under the Supervision of

Dr. K. B. Asthana
Professor & Dean
Department of Law

Under the Maharishi School of Law

Maharishi University of Information Technology
Sitapur Road, P.O. Maharishi Vidya Mandir
Lucknow, 226013

May, 2024

Dedication

I dedicate this research to my beloved father Late. Mohd. Mohsin.

Declaration

I hereby declare that the work presented in this thesis entitled " **Personal privacy in cyberspace** " in fulfillment of the requirements for the award of Degree of Doctor of Philosophy, submitted in the Maharishi School of Law, Maharishi University of Information Technology, Lucknow is an authentic record of my own research work carried out under the supervision of **Dr. K. B. Asthana**. I also declare that the work embodied in the present thesis-

i) is my original work and has not been copied from any journal/ thesis/ book; and

ii) has not been submitted by me for any other Degree or Diploma of any University/ Institution.

Kamshad

Maharishi University of Information Technology
Lucknow

Supervisor's Certificate

This is to certify that **Mr. Kamshad** has completed the necessary academic turn and the swirl presented by him is a faithful record is a bonafide original work under my guidance and supervision. He has worked on the topic **"Personal Privacy in Cyberspace"** under the School of Law, Maharishi University of Information Technology, Lucknow.

Dr. K. B. Asthana
Dean, Maharishi Law School
Maharishi University of Information Technology

Date: 11-05-2024

Acknowledgement

After intensive research and writing, the accomplishment of my thesis is realized. I very gratefully acknowledge the assistance of many people who helped and guided me, directly and indirectly, to fully enjoy and accomplish this research work. In the first place I am very thankful to God because without his blessings and invaluable guidance this task was just next to impossible for me to pursue. It was his invisible and memorable guidance because of that I received immortal support and blessings from many people.

It is my pleasure to express my deep gratitude to my supervisor. I found a wonderful and amazing person in the form of Supervisor; Prof. (Dr.) K. B. Asthana (Dean, School of Law) Maharishi University of Information Technology. He has been there to help me since the very first day of my research in a very pragmatic way.

I sincerely want to thank Dr. Trapty Agarwal, Dean Academics at Maharishi University of Information Technology, for her constant support and wonderful cooperation. The successful completion of this work would have been very difficult without the blessings.

Last but not least, I do not have enough words to express how grateful I am for the endless support of my family members. My father, Late Shri Mohd. Mohsin and mother Smt. Musarrat Jahan who has always provided me with unconditional love, and support. Without their faith in me, I could not have made it this far. This acknowledgement would be incomplete without showing gratitude to my sisters for their invariable support, love and blessings.

Above all finally, and most importantly, I would like to express deep gratitude to Shri. Varun Shrivastava, Shri. N. Das Mohapatra, Shri. Sandeep Sharma & Shri. Shivam Yadav for their unconditional support.

Kamshad

Abstract

The digital age has revolutionized the way individuals interact, communicate, and conduct their daily lives. With the proliferation of digital technologies and online platforms, the issue of personal privacy in cyberspace has become increasingly critical. This PhD thesis delves into the multifaceted dimensions of personal privacy in the digital age, aiming to provide a comprehensive understanding of its significance, challenges, and implications.

The research objectives of this study are twofold: firstly, to delineate the concept of the right to privacy in cyberspace, and secondly, to critically analyze the reality of personal privacy online. Through a meticulous examination of relevant literature, legal frameworks, and case studies, this research endeavors to shed light on the complexities surrounding personal privacy in the digital realm.

The study begins with an exploration of the origin and development of the right to privacy, tracing its evolution from historical and philosophical perspectives to its contemporary manifestations in the digital age. Special emphasis is placed on the comparison of privacy laws across different nations, with a particular focus on the Indian context.

One of the central themes explored in this thesis is the intersection between the right to privacy and other fundamental rights, such as freedom of speech and expression. The research investigates the delicate balance between these rights and the implications for individual liberties and social cohesion.

Furthermore, the study examines the implications of electronic surveillance and data breaches on personal privacy, highlighting the risks and challenges posed by these phenomena. Through a critical analysis of legal and ethical considerations, the thesis seeks to identify gaps in existing regulatory frameworks and propose recommendations for enhancing privacy protections in cyberspace.

The methodology employed in this research involves a combination of critical analysis and doctrinal approach, drawing on both primary and secondary sources of information. Primary sources include legal texts, judgments, and legislations, while secondary sources encompass scholarly literature, articles, and online resources.

The findings of this study underscore the importance of personal privacy as a fundamental human right in the digital age. The implications of the research extend

beyond theoretical considerations to practical recommendations for policymakers, technology companies, and individuals alike.

In conclusion, this PhD thesis contributes to the ongoing discourse on personal privacy in cyberspace by offering insights into its conceptual underpinnings, legal implications, and practical challenges. By fostering awareness and understanding of these issues, this research aims to empower individuals to navigate the digital landscape with confidence and autonomy.

Key Words: - Personal privacy, Cyberspace, Digital age, Right to privacy, Online privacy, Data protection, Surveillance, Freedom of speech, Electronic communication, Legal frameworks, Ethical considerations, Data breaches, Regulatory challenges, Comparative analysis, Indian context, Human rights, Privacy laws, Digital ethics, Information security, Policy recommendations.

Table of Contents

List of Abbreviation

A.C.	–	Appeal Case
A.LR	–	All India Reporters
A.P.	–	Andhra Pradesh
Ala.	–	Alabama
AOL	–	America Online website
ATM	–	Automated Teller Machine
C.P.C	–	Civil Procedure Code
CBI	–	Central Bureau of Investigation
CERT	–	Computer Emergency Response Team
Cr.P.C	–	Criminal Procedure Code
Del.	–	Delhi
DNA	–	Dioxin Ribo Nucleic Acid
E.g/e.g	–	Exempli Gratia
FBI	–	Federal Bureau of investigation
HC	–	High Court
HLR	–	Harvard Law Review
HTTP	–	Hyper Text Transfer Protocol
I.P.C	–	Indian Penal Code
ID	–	Identification
J.	–	Justice
J&K	–	Jammu and Kashmir
Jour	–	Journal
M.P	–	Madhya Pradesh
NPR	–	National Population Register
PIO	–	Public Information Officer
RBI	–	Reserve Bank of India
RBI	–	Reserve Bank of India
RTI	–	Right to Information
SC	–	Supreme Court
SSL	–	Secure Sockets Layer
T.N.	–	Tamil Nadu
TCP/IP	–	Transmission Control protocol/Internet Protocol
U.K.	–	United Kingdom
U.P.	–	Uttar Pradesh
U.S.A.	–	United States of America
UAV	–	Unmanned Aerial Vehicles
UIDAI	–	Unique Identification Authority of India
UN	–	United Nations
URL	–	Uniform Resource Locator
USB	–	Universal serial Bus
XSS	–	Cross Site Scripting

List of Cases

- Binoy Viswam v. Union of India 2017 SCC Online SC 647.
- Bird. v. Jones (1845) 7 QB 742 , 752 .
- Board of Revenue, Madras v. R. S. Jhavar AIR 1968 SC 59
- Bodhisatha Gautam v. Subhra Chakraborty AIR 1996 Supreme Court 922:(1996) 1 Supreme Court Cases 490
- Bombay Dyeing and Wfs. Co.Ltd (3) v. Bombay Emital Action Group (2006)3 Supreme Court Case 434, 510.
- Bonnard v. Perrryman (1891) 2 Ch 269.
- Bowers v. Hardwick 478 U.S. 186,211 (1986)
- Budh Singh v. State of U.P. (2006) 9 Supreme Court Case, 731, 738.F
- Byrne v. Kinematograph Renters Society (1958) 1 WLR 762
- Campbell v. MGN Ltd 2004 UKHL 22 : (2004) 2 AC 457 .
- Canada (House of Commons) v. Vaid 1 S.C. 667(2005)
- Canara Bank v. Central Information Commission AIR 2007 Ker. 225
- Carey v. Population Services International 431 U.S. 678(1977)
- Cassidy v. Daily Mirror Newspaper Ltd (1929) 2 KB 231: 141 LT 404.
- Chairmam, Railway Board V. Chandrima Das (2000) 2 Supreme Court Case465.
- Chandrakant Kalyandas v. State of Maharashtra (1969) 2 SCC 687: AIR 1970SC 1390.
- Cleveland Board of Education v. La Fleur 414 U.S. 632 (1974)
- Coben v. Cowles Media Co. 501 US 663,669 (1991)
- Common Cause (A Regd. Society) v. Union of India Civil Original Jurisdiction, Writ Petition (Civil) No. 215 Of 2005, decided on March 09,2018,
- D. Rajeshwari v. State of Tamil Nadu 1996 CRILJ, 3795.
- D.B.M. Patnayak v. State of A.P AIR, 1974 Supreme Court 209.
- D.K. Basu v. State of West Bengal (1997) 1 Supreme Court Cases 260.
- Dagg v. Canada 2 D.L., R 148(1997).
- Danik Bhaskar v. Madhusudan Bhaskar AIR 1991 MP 162, p. 166.
- Davis v. McArthur 17 DLR 760(1971).
- Deena v. Union of India, AIR 1983 SC 1155.
- Department of the Air Force v. Rose 425 U.S. 352(1976).

- Dharam Dutt v. Union of India AIR 2004 Supreme Court 1295.
- District Registrar and Collector v. Canara Bank AIR 2005 SC 186.
- Dixon V. Hoden (1869) LR 7 Eq 488
- Doe v. Balton 410 US 179 (1973).
- Door Das v. Manohaur Das - N.W.P.H.C. Rep. 1867, 269
- Dovaston v. Payne (1795) 22 HB 527.
- Dr. Nisha Malviya and Another v. State of M.P 2000 CRILJ, 671.
- Eisenstadt v. Baird 405 U.S. 438 (1972).
- Entick v. Carrinton (1765) 19 st Tr 1066.
- Foe vs. Uilman (1960) 36 7 U.S. 497 at 52
- Francis Coralie Mullin v. Union Territory of Delhi AIR 1981 Supreme Court746.
- Francis Coralie v. Union Territory of Delhi AIR 1981 SC 746.
- Frith v. Associated Press (DC SC) 176 F Supp. 671.
- G.R. Rawal v. Director General of Income Tax (Investigation) Appeal No.CIC/AT/A/2007/00490
- Ganeshilal v. Rasul Fathima AIR 1977 All. 118
- Girish Ramchandra Deshpande v. Central Information Commissioner (2013) 1SCC 212
- Gobind v. State of M.P AIR 1975 2 Supreme Court Case 148.
- Gokal Prasad v. Radho ILR 10 All. 358 (1888) at p. 384.
- Gouttam Kundu v. State of West Bengal AIR 1993 Supreme Court 229
- Govind v. Harilal AIR 1942 Bom. 217
- Griswold vs. Connecticut 381 U.S 479(1965)
- Grobbellar v. News Group Newspapers Ltd ; (2001) 2 All ER 437 (CA).
- Gulab Chand v. Manikchand AIR 1963 MP 63
- Gulam Mohd. v. Aziz Sheikh AIR 1966 JK 49.
- Gunga Pershad v. Sallk Pershad S.D.A.N.W.P. Rep. 1862 Vol. II, 217
- Harrison v. Duke of Rutland (1893) I QB 142.
- Harvinder Kaur v. Harminder Singh AIR 1984 Delhi 66.
- Hickman v. Maisey (1900) 1 QB 752
- Himachal Pradesh v. Umed Ram AIR 1986 SC 847

- Hinch Lal Tiwari v. Kamla Devi (2001) Supreme Court Case 496, J01.
- Hukum Chand Shyamlal v. Union of India AIR 1976 Supreme Court 789, 793;(1976)2 Supreme Court Cases 128.
- Hunter v. Southam 2 S.C., R 145(1984)
- Hussainara v. Home Secretary, Bihar(II) AIR 1979 Supreme Court 1360.
- In Re: Ramlila Maidan Incident Dt. 4/5.06.2011 v. Home Secretary, Union ofIndia and others,
- Jane Roe v. Henry Wade (1973) 35 L.Ed. 2d 147.
- Jivraj v.Keshayji AIR 1952 Kutch 22
- Joginder Singh v. State of U.P. AIR 1994 Supreme Court 1349
- Justice K.S. Puttaswamy v. Union of India and Ors. Writ petition (civil) no.494 of 2012. Decided on 24/09/2017.
- Justice Vicente v. Mendoza Supreme Court, 79 PHIL. L. J. 876, 876 (2004)
- K. V. Ramaniah v. Special Public Prosecutor AIR 1961 AP 190.
- Kadra Pahadya V. State of Bihar AIR 1981 Supreme Court 939
- Kaleidscoe (India (P) Ltd.) v. Phoolan Devi AIR 1995 Delhi 316., ILR 1996Delhi 586.
- Kartar Singh v. State of Punjab (1994) 3 Supreme Court Cases 569,638. Kattabomman Transport Corporation Ltd. v. State Bank of Travancore AIR1992 Kerala 351.
- Katz v. United States (1967) 389 U.S. 347.
- Keshav Sahu v. Dashrath Sahu AIR 1961 Orissa 154
- KF Media Inc. v. Vancouver (police department) 2 N.Z.L., R 728(1995).
- Kharak Singh v. State of Uttar Pradesh AIR 1963 Supreme Court 1295.
- Khatri v. State of Bihar AIR 1981 Supreme Court 929
- Khushwant Singh v. Maneka Gandhi AIR 2002 De 158.
- Kunwar Radha Krishan v. H. S. Bates (1951) ALJ 268.
- Lata Singh v. State of Uttar Pradesh AIR 2006 Supreme Court 2522
- Lavigne v. Canada (Office of the Commissioner of Official Languages), 214D.L., R215(2000)
- Laxmikant V. Patel v. Chetanbhat Shan AIR 2002 Supreme Court 275.
- Lokniti Foundation v. Union of India Civil Original Jurisdiction, Writ

Petition(C)No.607 Of 2016, Supreme Court of India, ordered on February 6, 2017.

- London Artists Ltd v. Litteler (1968) WLR 607, 615
- Loving v. Virginia 388 U.S. I (1967).
- Lyons v. Wilkins (1899) 1 Ch 255.
- M. H Hoskot v. State of Maharashtra AIR 1978 Supreme Court 1548
- M. Vijaya v. Chairman and Managing Director, S. C. C. Ltd AIR 2001 AndhraPradesh 502.
- M.P.Sharma v. Satish Chandra AIR (1954) 300, SCR 1077.
- M.S.M. Sharma v. Shri Krishnan Sinha AIR 1959 Supreme Court 395, 410-11.
- Maharaj Kumar Mohammad Husan Khan v. Hafaz Abdul Hague AIR 1945Avadh 15.
- Maharashta V. Praphaks Pandurag AIR 1966 Supreme Court 424.
- Makhan Singh Tarsikka V. State of Punjab 1952 SCR 368.
- Malak Singh v. State of P&H AIR 1981 SC 760.
- Maneka Gandhi v. Union of India AIR 1978 Supreme Court 597.
- Manlklal v. Mohanlal AIR 1920 Bom. 141
- Mata Prasad v. Blhari Lai S. A. No. 8 of 1856
- Mayer v. Nebraska 262 U.S. 390,399(1923).
- Maynard v. Hill 125 U.S. 190, 211 (1888) Megraj Patodia v. R. K. Birla(1971) IS.C.R.399.
- Milk Wagon Drivers Union V. Meadowmoor 312 U.S 287(1941)
- Miller v. California 38 L Ed 2d 128: 413 US 15 (1972) 413 US 25 (1973)
- Mitha Rustom ji Murzban v. Nusserwanji Engineer (1941) 43 Bom LR 631.
- Mohan Lal Sharma v. State of U.P (1989) 2 Supreme Court Cases 314.
- Moore v. City of East Cleveland 431 U.S. at 505-06. Moorefield v. U.S. SecretService 449U.S. 909(1980)
- Mr. ‘X’ vs. Hospital ‘Z’ (1998) 8 Supreme Court Cases 296 .
- Mst. Ramdhara v. Mst. Phulwatibai 1969 MPLJ 483.
- Mukesh Kumar Ajmera v. State of Rajasthan AIR I 997 Raj 250
- Mukund Martand Chitis V. Madhuri Chitnis AIR 1992 Supreme Court

1804.

- Munn v. Illinois 94 U. S. 113 (1877)
- Murari Mohan Koley v. The State and Another (2004) 3 CALLT 609, HC
- MX of Bombay Indian Inhabitant v. M/S ZY. AIR 1997 Bom 406.
- NAACP v. Alabama 357 U.S 449(1958)
- Nagesh Ganesh Patil S. v. Public Information Offices, SBI, Bandra, MumbaiRTIR II (2013) 9 (CIC).
- NALSA v. Union of India AIR 2014 SC 1863
- Nand Kishore Sharma v. Union of India 2005 Indlaw Raj 142.
- Nandani Satpatti v. P. L Dani AIR 1978 Supreme Court 1025 at 1045.
- Narinderji Singh Sahni V. Union of India (2002) 2 Supreme Court Cases 210,237,3Q
- National Treasury Employees Union v. Von Raab 109 S.Ct. 1384 (1989)
- Navtej Singh Johar v. Union of. India (2018) 1 SCC 791
- Naz Foundation v. Government of NCT of Delhi 2010 Cri.LJ 94 (Del.).
- Near v. Minnesota Ex Rel. Olson Supreme Court of USA, 1930. 283, 697, 51S. Ct. 625, 75 L. Edition. 1357.
- Neera Mathur v. Life Insurance Corporation of India AIR 1992 Supreme Court264(Para 28(2)) 6 Supreme Court Cases 632.
- Niemietz v. Germany, ECHR 16 june 1992, Series A no. 251-B,33
- Nigamma v. Chikkaiah AIR 2000 Kant 50.
- Noor Mohd. v. Mohd. Jiauddin AIR 1992 MP 244.
- Nuth Mull v. Zuka-OoUah Beg S. D. A. N.-W. P. Rep., 1855, p. 92.
- Obergefell v. Hodges 576 United States 644 (2015).
- Olmstead v. United States 277U.S 438(1928)
- Ontario (A.G.) v. Dieleman 117 D.L., R 680(1994).
- P. Rathinam v. Union of India AIR 1994 SC 1844.
- P.D. Shamdasani v. Central Bank of India AIR 1952 Supreme Court 59 Paardarshita Public Welfare Foundation v. Union of India and Ors., AIR 2011Del. 82.
- Paduinadas v. Smt Parwati AIR 1985 All. 648.
- Palko v. Connecticut 302 US 319 (1937).
- Paul Singh v. State of Haryana AIR 1980 Supreme Court 249.

- Peoples Union of Civil Liberties (PUCL) v. the Union of India 1 SupremeCourt Cases 301: AIR 1997 Supreme Court 568.
- Peoples Union of Civil Liberties v. the Union of India AIR 2003 SupremeCourt 2363.
- Peoples Union of Civil Liberties v. the Union of India AIR 2004 SupremeCourt 1442.
- Peter Semayne v. Richard Gresham (1603) 5 co. Rep. 91 , 916.
- Planned Parenthood of Missouri v. Danforth 428 U.S. 52(1976)
- Poe v. Ullman 367 U.S 497(1961)
- Pooram Mai v. Director Inspection AIR 1974 SC 348.
- Popatlal Gokaldas Shah v. Ahmedabad Municipal Corp. AIR 2003 Guj 44.
- Prem shanker v. Delhi Administration AIR 1980 Supreme Court 1535.
- Quartz Hill Con. Mining Co. v. Beall (1882) 20 Ch. D 501
- Quoting Skinner v. Oklahoma 316 U.S. 535, 541 (1942)
- M. Malkani v. State of Maharashtra AIR 1973 SC 157
- R.C. Cooper v. Union of India AIR, 1970 Supreme Court 564, (1970) 3 SCR530 .
- R.K. Jain v. Union of India (2013) 14 SCC 794
- R.M. Malkani v. State of Maharashtra AIR 1973 Supreme Court 157.
- R.Rajagopal v. State of Tamilnadu (1994) 6 Supreme Court Case 632.
- Rabonwitz v. U.S 339 U.S.50 (1967)
- Rajan Verma v. Union of India, Ministry of Finance, Banking Division, NewDelhi 2008 (2) Supreme Court Cases 335 (P&H).
- Ram Baksh v. Ram Sookh N.W.RH.C. Rep. 1868, 253
- Ram Jethmalani v. Union of India (2011) 8 SCC 1.
- Rama Reddy v. V. V. Giri AIR 1968 SC 147
- Ramchandra Ram Reddy v. State of Maharashtra 1 (2205) CCR 355 (DB)
- Ramjethmalani v. Union of India (2011) 8 Supreme Court Cases 1.
- Ranjit D. Udeshi v. State of Maharashtra AIR 1965 SC 881
- Reliance Industries Ltd. v. Gujarat State Information Commission AIR 2007Guj. 203
- Roach v. Harper 143 W. Va860, 105 SC 2d 564 Robbins v. CBC

Robbins 12DLR 32(1957).

- Roberts v. United States Jaycees 468 U.S. 609 (1984)
- Roe v. Q J Wade 405 U.S. 438 (1972).
- Rosenbhatt v. Baer, 383 U.S. 75(1966)
- Rosenbloom v. Metromedia, 403 U.S. 29(1971)
- Khusboo v. Kanniammal 2010 5 SCC 600
- S.P.S Rathore V. C.B.I. 2010(3) RCR 325
- Saifiidin Saheb v. State of Bombay AIR 1962 SC 853.
- Santosh Singh V. Delhi Administration AIR 1973 Supreme Court 1091.
- Saroj Rani v. Sudarshan Kumar AIR 1984 S 1526
- Satwant Singh v. A.P.O AIR 1967 Supreme Court 1836.
- Selvi v. State of Karnataka (2010) 7 SCC 263
- Sewakram Sobhani V. R.K. Karanjiya 1981 Cri. L. J. 894.
- Shapiro v. United States 335 U.S. 1(1948)
- Sharda Singh v. State of U. P. 1999 Cri. L. J. 188 (All).
- Sharda v. Dharampal, 2003 AIR Supreme Court W 1950.
- Sheela Barse v. State of Maharashtra AIR 1983 Supreme Court 379
- Shri Krishna Murthy v. U. Ramlingam AIR 1980 Andhra Pradesh 69.
- Shri Rakesh Kumar Singh v. Lok Sabha Secretariat Complaint No. CIC/WB/C2006/00223; Appeal Nos. CIC/WB/A/2006/00469; & 00394
- Sim v. Strech All ER 1237, (1240).
- Skinner v. Railway Labor Executives' Association 489 U.S. 109 S.Ct. 1402(1989)
- Smt Gian Kaur v. State of Punjab AIR 1996 Supreme Court 946.
- Smt. Saroj Chotiya v. State of Rajasthan AIR I 998 Raj 28.
- Sri Bhagwan Ramchandraji v. Babu Purshottamdas Second Appeal No. 191 of1959. Decided on 25.11.1960
- Stanley v. Georgia 374 U.S. 557(1969).
- State of Andhra Pradesh v. Gangula Satya Murthy AIR 1997 SC 1588
- State of Bombay v. Kathi Kalu Oghad AIR 1961 SC 1808
- State of Maharastra v. Christian Community Welfare Council of India (2003)8 Supreme Court Cases 546, 549 - 50 (Para 9).

- State of Maharastra v. Madhukar Narain AIR 1991 Supreme Court 207.
- State of Punjab v. Baldev Singh AIR, 1999 Supreme Court 2378
- State of Punjab v. Gurmit Singh AIR 1996 SC 1393
- State of Punjab v. Ramdev Singh AIR 2004 Supreme Court 1290.
- State of U.P. v. Ram Babu Misra AIR 1980 SC 791,1980 SCR (2)1067, (1980)2 SCC 343
- State of West Bengal v. Ashok Dey AIR 1972 Supreme Court 1660
- State v. Bhawani Singh AIR 1967 Del 208, 211 (FB).
- State v. Charulata Joshi AIR 1999 4 Supreme Court Case 65.
- Stepkens v. Myers (1830) 4 C & 349 .
- Subhash Chandra Agrawal v. Supreme Court of India File No. CIC/WB/A/2006/00460 decided on 14 August 2020
- Suchitra Srivastava and Anothers v. Chandigarh Administration AIR 2010 SC236.
- Sunil Batra v. Delhi Administrative AIR 1978, Supreme Court 75
- Sunkara Satyanarayana v. State of Andhra Pradesh (1999) 6 ALT 249.
- Suresh Kumar Koushal v. NAZ Foundation and others (2014) 1 SCC 1.
- Surjit Singh Thind v. Kanwaljit Kaur AIR 2003 P& H 353
- Suxam Teli v. Bipal Teli (1905) 4 CLJ 388.
- Sareetha v. T. Venkata Subbaiah AIR 1983 AP 356.
- Terry v. Ohio 392 U.S.I. (1968).
- Thogorani Alias K. Damayantivs v. State of Orissa and Ors 2004 Cri L J4003(Ori)
- Union of India v. Association for Democratic Reforms and Another AIR 2002SC 2112
- Unique Identification Authority of India (UIDAI) v. Central Bureau ofInvestigation (CBI) SLP (Crl) 2524/2014, Supreme Court of India
- United States Department of justice v. Reporter's Committee for Freedom ofthe Press 489 U.S. 749(1989).
- United States v. Karo 468 U.S. (1984) United States v. Knotts 460 U.S. (1983)United States v. Miller 425 U.S. 425(1976).
- V. Krishnan v. G. Rajan H.C. M.P. No. 264 of 1993.

- Victoria Park Racing Co. v. Taylor (1937) 58 CLR 479.
- Vidya Verma v. Shiv Narain Verma 1955(2) SCR 983.
- Vijay Prakash v. Union of India AIR 2010 Del. 7
- Vishaka v. State of Rajasthan AIR 1997 Supreme Court 3011.
- Wandsworth Board of Works v. United Telephone co.(1884) 13 QBD 904,927.
- Wolf v. Colorado 338 U.S. 25(1949)
- Yousoupoff v. Metro Goldwyn Mayer Pictures Ltd (1934) 50 TLR 581, 587:78 SJ 617.
- Yusuf Ali Ismail Nagree v. State of Maharashtra AIR 1973 SC 157.
- Zablocki v. Redhail 434 U.S. 374 (1978).

Chapter-1

Introduction

Privacy includes a composite of interface, which require protection by the lawful framework. Developments in the field of Information and Communication Technologies (ICT) have transformed human life as well as communication and interactions between people throughout history. In modern times the Cyberspace makes these interactions and communication possible and people can communicate and do business and commercial activities without taking into account the political boundaries and distances due to advent of ICT.

Cyberspace is the creation of human beings and it has incredible effects on our life including human rights and freedom of speech and expression, right to privacy. ICT has made our life easy at same time it has new threats for people, business and governments. Power of the State to cause surveillance over people has widely been criticized as it has negative impact on human rights.

Cyberspace is the basis of all activities in cyber world. Cyber world is a new phenomenon. It contains an online environment in which people may operate as simply and freely as they do in actual circles in commercial and private activities. The free dictionary identifies the cyber world as the computer and communication world. It means the fast- moving world of high technology today.[1]

Since the cyber world is all based on cyberspace, it is important to appreciate the concept of cyberspace. It is interconnected technology. Cyberspace has been defined as consensual hallucination experienced daily by billions of legitimate operators. In the 1990s, the term "cyberspace" started to be popular with all the uses of the Internet, networking and digital communication that grew significantly and represented several new concepts and physics. It is the biggest unregulated and uncontrolled realm in human history.

[1] http://encyclopedia2.thefreedictionary.com/cyber world.

The term cyberspace has become a traditional method to define something related to the Internet and the various culture of the Internet. The cyber environment is characterized by the social interactions rather than its technological implementation, according to Chip Morningstar and F. Randall Farmer.[2] The computer medium in cyberspace is, according to them, an extension of the communication channel between actual people; the key feature of cyberspace is its capacity to impact and influence one another across the environment. This cyberspace has become an online forum for a galaxy of human activity. In fact, sometimes activities which are carried in cyberspace are illegal in nature.

Before analyzing data privacy in cyberspace, it is pertinent to go through the history of privacy. Although not specifically present in theory of law, data protection interest can be found in philosophical and legal thinking and justified. To define the idea of confidentiality is of little benefit from the works of the great liberals, as confidentiality is an ignored virtue and remains understood by the great liberal thinkers.

Even in the USA and in England, their legal acknowledgement has been gradual. In 1890, Samuel Warren and Louis Brandeis wrote an article of law in 1890 and the legal idea came about6 and published a law article in 1890. The pair was an existent common law right that incorporated the protection of "inviolable personality" for each individual. From the period of their concepts the genesis of this legal notion is unclear. Although the right to privacy was acknowledged as another legislative chapter following legal writings, it was defined by the judiciary a number of times. The Human Rights Act 1998 includes the Convention on Human Rights and Fundamental Freedoms, which was signed in 1950 as a British statute. Article 8[3] of the European Convention for Human Rights, 1953 stipulates that everybody has the right of his house and communication, to respect for his private and family life. The Universal Declaration of Human Rights in Article 12[4] states that: “No one shall be subjected to arbitrary

[2] Morningstar, Chip and F. Randall Farmer. The Lessons of Lucasfilm's Habitat. The New Media Reader. Ed. Wardrip-Fruin and Nick Montfort: The MIT Press, 2003. 664-667.

[3] Everyone has the right to respect for his private and family life, his home and his correspondence.

[4] No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks

interference with his privacy, family, home or correspondence, or to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks". Article 17(1) of the International Civil & Political Rights Pact (1966) says that no-one shall be litigated against his privacy, family home, letters, or illegal assaults on his honour and character, the provisions of Article 17(1) of the Convention shall be applicable. Article 11 of American Convention on Human Rights provide for right to privacy, household privacy, professional privacy, medical privacy, financial privacy etc.

Privacy could be a natural require of a man to set up individual boundaries and to confine the passage of others into that region. There are adequate evidences in both oriental and occidental civilizations to bolster this see. The roots of right to privacy may be followed back from the natural rights, which are basic, inherent and unavoidable rights. There are too solid lawful bases for the right to privacy in International Law. Article 12 of the Universal Declaration of Human Rights,1948, Article 14 of the International Covenant on Civil and Political Rights, 1966, Article 16of Convention on Rights the Child of the United Nations, 1989, Article 14 of the United Nation's Convention on Migrant Workers, 1990 to talk almost the right to Privacy.

In India, in spite of the fact that this right isn't explicitly said within the Constitution, it is translated by the Supreme Court to be inferred within the Article 21 of the Indian Constitution. The right to privacy in India has created through a series of decisions over the past 61 years. This has been reiterated in a number of cases such as *M.P.Sharma* v. *Satish Chander*,[5] *Kharak Singh* v. *State of Uttar Pradesh*,[6] *Gobind* v. *State of Madhya Pradesh*,[7] *R.Rajgopal* v. *State of Tamilnadu*, [8] *Peoples Union of Civil Liberties* v. *Union of India*,[9] *Justice K.S. Puttaswamy* v. *Union of India and Ors*.[10] and *Subhash Chandra Agrawal* v. *Supreme Court of India* [11] "The Constitution Bench of the Supreme Court of India held that the Supreme Court is a 'public authority' andhence will fall within the ambit of the Right to Information Act, 2005 (RTI Act). The

[5] AIR (1954) 300, SCR 1077.
[6] AIR (1963) 1295, SCR (1) 332.
[7] AIR (1975) 1378, SCR (3) 946.
[8] AIR (1994) 6 SCC 632.
[9] AIR (1997) 1 SCC 301.
[10] (2017) 10 SCC 1.
[11] File No. CIC/WB/A/2006/00460 decided on 14 August 2020.

respondent, Subhash Chandra Agarwal, an Indian businessman and right toinformation activist, filed separate applications requesting access to information fromthe Central Public Information Officer (CPIO) relating to assets of sitting judges, as well as correspondence relating to the appointment of judges and alleged influence on a decision. The applications were denied with a response that the information requested was either exempted or confidential. Upon appeal, the Chief Information Commission (CIC) granted access to the information. The appeal against one of the orders before the Delhi High Court led to a judgment from its Full Bench holding theOffice of the Chief Justice of India to be a public authority and subject to the RTI Act.The Court conducted a proportionality test, balancing the right to privacy against the public interest in disclosure, to find that the requested information regarding the functioning of the Supreme Court and judicial assets should be released in the name of transparency and accountability, but that information related to third-parties neededto be re-examined[12]. The Apex Court acknowledged the privacy infringements in thesecases. The right to privacy is protected as intrinsic part of the right to life and personalliberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution."

In India right to privacy is not directly dealt with in the constitution. It does not participate in discussions of the Constituent Assembly. The Constituent Assembly explicitly rejected a suggestion to include a clause such as the Fourth Amendment to the U.S. Constitution which is at the foundation of the U.S. privacy legislation forbidding, improper searches and seizures. Therefore, when the right exists, it must be placed within the constitutional structure as expressed in the court statements. The provision like freedom of speech and expression7 and right to life and personal liberty8 has its effect to the right to privacy as a fundamental right. Right to privacy brought under Art 21 of the Indian Constitution by bringing various rights by the Supreme Court of India. Private rights are a unique and independent notion which has been created as an act for damages caused by unlawful invasion of a person's privacy under tort law. This right has two sides, two sides of the same coin: (1) a general law that allows damages caused by the illegal invasion of data security, and (2) a constitutional recognition of the law that safeguards personal privacy against the illegal invasion of the Government.

[12]https://globalfreedomofexpression.columbia.edu/cases/central-public-information-officer-supreme-court-of-india-v-subhash-chandra-agarwal/. Visited on 25th of January 2023.

The Right to Privacy has assumed much importance with the emergence of internet, bio-banks (gene bank etc.) business process outsourcing, knowledge process out sourcing, development of software industries, enactment of antiterrorist laws, deterioration of the law and order situation, rising levels of crime rates (theft and fraud cases etc.).[13] These developments led to the rampant privacy invasions. "Despite its legal guarantee as a basic human right, it is invasions incessantly by the individuals and institutions. The internet has penetrated into every sphere of human activity. It is intricately and inextricably connected with the day-to-day life of the present day. Modern man's life has been changed drastically and all his transactions have become more internet-based, internet-dependent in this global village. Personal information of an individual in this internet age is not just confined to four walls, or in our traditional desk, but is connected to the vast networked internet system. This is leading to privacy invasions. Most of our day-to-day transactions (financial, medical, school/college etc.) are no more secure now. Our personal information is tracked, stored and later is- utilized in the manner we do not wish often without our knowledge or consent. The law enforcing authorities to, under the veil of combating terrorism are infringing the innocent individual's Right to Privacy through their acts such as phone tapping, surveillance of private lives and searches and seizures without complying necessary legal formalities etc. Today's technology gives the media powerful new tools for intrusion into private lives. Cameras are smaller and easier to hide. Conversations are easily recorded surreptitiously. Computers and the Internet provide the ability to rummage the closets of your life in ways that have never before possible. Many suits against the media now claim invasion of privacy, not libel. Jurors have strong feelings in this area. So do judges. Privacy cases focus on personal, emotional beliefs in conflict with each other. We inherited criminal trespass from British Common Law. But that protects your real estate from intrusion. The idea of a right to privacy in your personal life was not even conceived until the 1890s when newspapers became more sensational with stories of gossip and sexual scandal". They even published pictures, which do nothing with a public interest.

"The paparazzi are photographers who will certainly do anything to achievetheir aim in gaining the profit from the photos of famous people and their families. They sell the

[13] Warren and Brandeis, "The Right to Privacy", 4 Harvard Law Review, 193 (1890).

photos to tabloids or anyone else who is willing to pay them a high price.The word paparazzi were first released on Italian film 'La Dolee Vita' in 1960. La Dolee Vita, it was the story of one tired journalist, Marcello and his photographer, Paparazzo. Federico Fellini who was director of the film describes the word of paparazzo: Paparazzo suggests to me a buzzing insect hovering darting stinging. Moreover, Fellini drew a picture of the paparazzo's character that looks like a vampirish insectile, implied that paparazzi are like mosquitoes and also parasites. Afterthat Paparazzi is a word to explain the behavior of photographers who chase up the celebrities to get the information about them to reveal in the public the same as the acton film"[14].

As we see from some of the celebrity's cases who are a victim of the hunter in the name of paparazzi. "There are many reproaches against paparazzi of their behavior ravaging into the society. Someone proposes to issue a law to prevent and limit the terrible danger that may happen when the paparazzi follow the celebrities. It is not wrong for photographers to take pictures of the famous people but it is wrong totake pictures without their permission. The lack of privacy and human right realizationof media may cause the paparazzi problem".

The Unique Identification Number has been depicted to be a new face of development that technology could bring about. "It has been sold to masses in India asa solution for accessibility to the service delivery and as a tool for the eradication of ill governance, but there are issues of larger importance that have gone unnoticed. These include the privacy and dignity of an individual being affected by the UID scheme. UID is a product of what started as an idea of biometric identity cards for theBorder States in India in the wake of the increased terrorist activity. The consulting agency suggested that the identity cards could be implemented in the entire country. Now the government is trying to implement the new UID scheme by making it as a development agenda. The deeper question of surveillance by the State and invasion ofprivacy at all levels arise as a result of the UID project. All the data pertaining to an individual could be accessed at one time. This could lead to a situation where an individual's autonomy could be severely compromised. It is evident that the UID scheme could lead to providing more power to the hands of the State. We should not forget that the Rwanda genocide it was by using identity cards that the demarcation ofthe Tutsis and Hutus could be done".

[14] https://dictionary.cambridge.org. Visited on 20th of February 2022.

"The main privacy concerns brought by the UID projects are territorial and data privacy. Territorial privacy addresses freedom from encroachment in domestic and official spaces by the way of surveillance. Identity and information privacy or dataprivacy deals with the protection of information, especially sensitive information. It isimportant to note here that the concept of privacy in the social sphere is not as prevalentas it is in Europe or the United States. It is relevant to quote here from the famous article on privacy by Warren and Brandeis."[15]

Recently in the context of the development of a right to privacy, the Unique Identification Authority of India (UIDAI) has been established by the Government of India in February 2009. "The main objective of this project is to provide an identity for everyone a database for residents of the country in the form of very simple biometric data. Such a project in India is known as Adhar. The Adhar has 12–digit number and it is unique for every citizen. Its main object is to link the basic demographics and biometric information such as iris, fingerprints, and photograph of the citizens[16]. Lately its inception as the flagship program of the Unique IdentificationAuthority of India (UIDAI), the Aadhaar scheme, has undergone scrutinizes and challenges at various levels including the pending challenges in Supreme Court and the heated debates in the Parliament over the Aadhaar Bill, 2016 (now the Aadhaar Act). The Aadhaar (Targeted Delivery of Financial & Other Subsidies, Benefits & Services) Act, 2016 (hereinafter called the Aadhaar Act) was notified in the Gazette of India on March 25, 2016. The principal purpose as explained by finance minister while introducing the Bill is to empower the state to distribute the resource of the stateto the deserving people and save revenue so that it does not go to undeserving people.However, the provisions allowing identification of an individual, disclosure of information and use of identity information by private entities have made the object ofthe Act difficult to understand. The focus of this paper is on the debate in the parliament regarding the provisions of the Bill and pointing out certain issues in the Act from a legal point of view". Thus, there is no discussion on the issue of Money Bill or the petitions that are pending in the court.

This is not legislation without flaws. "There is a lot that's left to be clarifiedthrough

[15] Warren and Brandeis, "The Right to Privacy", 4 Harvard Law Review, 193 (1890).
[16] https://uidai.gov.in/legal-framework/aadhaar-act.html. Visited on 25th of march, 2022 .

delegated legislation which the government is slowly doing by means of regulations. However, it cannot be denied that the UIDAI has got very wide powers to make regulations by virtue of section 54 of the Act[17].

The government has to be very careful with regard to the use of the information collected since the Act allows privateentities to perform any function given to them by a contract. Since its inception the Aadhaar scheme has been under scrutiny, therefore, there are many cases filed againsta different aspect of the scheme. The three major aspects are the right to privacy and the Act being passed as a Money Bill. The petitions with regard to these are still pending in the court. With regard to the nature of the scheme of Aadhaar the main argument of the government is that the services are voluntary but if a person wants toavail a service he should have Aadhaar, this really makes it rather mandatory in nature.The government has been regularly notifying the services for which Aadhaar is mandatory, the latest one is the mid-day meal scheme. The demerit of living in a digital world, privacy has become the biggest concern now, examples like Hillary Clinton's use of private email servers, the alleged Russian hacking of the Congress's server andmost importantly the NSA spying exposed by Snowden show us that the law, unfortunately, has not kept pace with technology. The same happened in the case of Aadhaar where the Act was passed a few years after the beginning of registration of Aadhaar. It must be noted that countries like China, Australia, the UK, and France have rejected similar identity schemes". Therefore, only time will tell whether the benefits of Aadhaar outweighs the risks involved.

Further The Data (Privacy and Protection) Bill, 2017, grants a statutory Rightto Privacy under Section 4[18]. However, "this Right to Privacy is only pursuant to Articles 19 and 21. While a statutory recognition of the Right to Privacy may be applauded for being a baby step in the right direction, is critical to appreciate the dangers of linking the same with Fundamental Rights under Articles 19 and 21, as thecontours of the Right to Freedom of Speech and expression and the Right to Life are malleable and colored by the decisions of the judiciary, keeping the socio-political reality of a period in mind.

[17] See The Aadhaar "(Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 Section 54.

[18] See The Data (Privacy and Protection) Bill, 2017 Section 4: - Notwithstanding anything contained in anyother law for the time being in force, pursuant to article 19 and 21 of the Constitution and subject to theprovisions of this Act, all persons shall have a right to privacy.

However, it is essential to note that this Bill applies not only to private corporations or body corporate but is equally applicable to state entities,government agencies or any other persons acting on their behalf. Even the definition of a 'third party' under this Bill includes in law from the existing regime under the existing Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011(SPDI Rules)".

Section 14 of the Bill stated that[19] "while giving consent, the person shall have a 'legitimate expectation' that the data controller/processor will abide by the provisions of this Act, who must take all security measures necessary for safeguardingsuch personal data with 'due diligence'. While the intentions of the Bill are to providea person with a safety net against data protection breaches, it is essential to elucidate the difficulty in matching such standards of protection as cyber-attacks and data thefts continue to evolve, often leaving existing security measures redundant. This may open the floodgates of litigation. The Bill also introduces the concept of pseudo- anonymisation of data, so that a person cannot be identified using such information without the use of additional data. However, pseudo-anonymisation has not been mandated but is only 'encouraged', leaving gaping loopholes especially in the context of protection of sensitive, personal data."

Under Section 36[20], no person can assist in or conduct surveillance of a person. However, "an exemption has been made for state agencies, subject to certain restrictions and prior approval by the DPPA. The time duration for storing such data must be specified and no data that is no longer necessary for the State agency can be accessed after a year from the DPPA's approval to ensure the states does not disrespecta person's right to Privacy. However, with respect to sensitive, personal data, Section 20(2)[21]

[19] See The Data (Privacy and Protection) Bill, 2017 Section 14. (1) Every person at the stage of giving consent for collection, processing, use or storage shall be have a legitimate expectation that data controllers and data processors shall abide by the provisions of this Act. (2) Data Controllers and/or Data Processors shall take all security measures necessary for safeguarding and securing the personal data in their custody with due diligence.

[20] See The Data (Privacy and Protection) Bill, 2017 Section 36. Except for the manner provided in this Actand the rules prescribed thereto, no person shall conduct or assist in conducting any surveillance of another person.

[21] See The Data (Privacy and Protection) Bill, 2017 Section 20. Notwithstanding anything contained in section 16 or section 19 of this Act, (2) No sensitive personal data under sub-section (1) shall be processed for any purpose apart from for the specific purpose for which it was collected and/or

provides that no sensitive data shall be processed for any other purpose apart from its intended use but can be used by welfare schemes and social protection laws.

Hence, this would imply that the Aadhaar scheme of BHIM (Bharat Interface for Money) would also have access to a person's personal, sensitive information. This Section is analogous with the present dispute at the Supreme Court and will continue to be subject to debate due to the existing privacy concerns".

The Personal Data Protection Bill, 2019 ("PDPB") was introduced in Lok Sabha by the Minister of Electronics and Information Technology, "on December 11, 2019. The purpose of this Bill is to provide for protection of privacy of individuals relating to their Personal Data and to establish a Data Protection Authority of India forthe said purposes and the matters concerning the personal data of an individual. The Bill proposes to supersede the Information Technology Act, 2000 (Section 43-A)[22] deleting the provisions related to compensation payable by companies for failure to protect personal data. The PDPB inter alia, prescribes the manner in which personal data is to be collected, processed, used, disclosed, stored and transferred".

The Personal Data Protection Bill, 2019 proposes to protect **"**Personal Data" relating to the identity, characteristics trait, attribute of a natural person and "Sensitive Personal Data such as financial data, health data, official identifier, sex life, sexual orientation, biometric data, genetic data, transgender status, intersex status, caste or tribe, religious or political beliefs. Pursuant to the PDPB being enacted into an Act, there are several compliances to be followed by organizations processing personal data in order to ensure protection of privacy of individuals relating to their Personal Data."

Consent of the individual would be required for processing of personal data. Based on the type of personal data being processed, organizations will have to reviewand update data protection policies, codes to ensure these are consistent with the revised principles such as update their internal breach notification procedures, implement appropriate technical and organisational measures to prevent misuse of data, Data Protection

implementation of welfare schemes and social protection laws.

[22] See The Information Technology Act, 2000 Section 43A:- Compensation for failure to protect data

Officer to be appointed by the Significant Data Fiduciary, and instituting grievance redressal mechanisms to address complaints by individuals.

Lastly, "the Bill has made all offences under its provisions cognizable offences and has increased the monetary penalty and imprisonment period for all existing breaches. Further, the concept of applying a high monetary penalty on a per day basis, based on a number of days of violation of data protection, has been imposed,to ensure defaulters are forced to take appropriate measures to remedy the breach on atimely basis. Hence, while this Bill introduces a few much-needed changes in terms ofexpanding the scope of applicability of data protection laws and recognizing the Rightto Privacy, such euphoric provisions are equally shadowed by sections that enable usage of sensitive, personal data for welfare schemes, thereby imposing a statutory limitation on the Right to Privacy".

1.1 Review of Literature

The researcher has scrutinized the accessible work of the Indian as well as outside authors on the subject. The researcher moreover overviewed the important case law relating to the subject. Advance, the researcher has gone through National and International Statutes, Reports of law Commissions, e-sources, daily papers, periodicals and Law Reports, Digests and Journals. The researcher has moreover gonethrough a few reference books to get it the recognition of the authors on the subject. The researcher has been gathering and analyzing the consider fabric accessible in numerous libraries.

Following is the selected review of some literature referred-

The book titled ***"Indian Constitutional Law"*** by **M.P Jain**, is used by the researcher as the base book to study the constitutional dimensions and judicialresponse to the right to life and personal liberty and further the interpretation of right privacy by the Hon'ble Supreme Court and High Courts.

The book titled ***"Facets of Media Law"*** by **Madhavi Diwan Gordia,** is another book referred to on the subject. The author of the book has clarified sufficienton the history of the media law in Indian legal system. He has specified a arrangementof cases, views, suppositions of the famous experts etc. This has encouraged the researcher to bolster his basic investigation of privacy. The cross-examination portionis the crucial part when

media criticism is in question; the author has clearly said all the pros and cons of it, which has once more made a difference the researcher.

The book titled ***"Constitutional Law of India"*** by **H.M. Seervai**,. The authorof this book maybe the leading commentary on the Constitution of India, lauded by the Bar and frequently cited by the Judiciary in judgments. This demonstrated of extraordinary offer assistance to get it and analyze the judicial drift in cases relating right to privacy and confinements of media freedom on privacy.

The book titled ***"Constitutional Law: Civil Liberty and individual Right"*** by **William Cohen & David J. Danelski's**, . This book has been truly much offer assistance since it made the researcher conceptually as well as substance shrewd clearalmost privacy. This book moreover has been supportive to get it privacy in America through Constitutional and Judicial advancements.

The book titled ***"Privacy Law-Principles, injunctions and compensation"*** by**Rishika Taneja, Sidhant Kumar,** is the authoritative book on the right to privacy. The idea of privacy, its scope and standards of privacy protection have been extravagantly talked about here. Authors embrace critical research by comparing the lawful premise of privacy in numerous nations and under international and territorial traditions. The book applies a few light on developing issues of interruption of privacythat emerges within the period of progressed data and communication. The pair authorshave comprehensively bargain with the practical approach of right to privacy concerning freedom of speech and expression including freedom of the press and public interests.

The book titled ***"Encyclopedia of Privacy"*** by **William G. Staples** has provedvery useful for understanding the concept of privacy in common law countries.

The book titled ***"Law and Protection of Right to Privacy"*** by **Jyoti J. Mozika**,is a comprehensive book on the right to privacy. The author endeavours to expand on different aspects of the right to privacy in its comprehensive centrality bordering on the different international law conventions, Supreme Court decisions of the United States and England additionally focalizing on Indian authoritative reactions and judicial professions. The author has judiciously outlined the right to privacy interfacing with numerous measurements and depicted the sorts of individuals for whom this rightbears awesome importance.

The book titled ***"The Right to Privacy in India Concept and Evolution"*** by **Ravinder Kumar**, this book is based on the early concept and subsequent evolution of the Right to Privacy in India. This book helps the researcher to understand the historical evolution and development of the law on privacy.

The book titled ***"Right to Information"*** by **S.P Sathe**, in his book, laid down that the right to freedom of speech and expression often collides with two rival rightsnamely the right to privacy and the right to fair administration of justice. Both the right is protected by the law of tort and contempt of court respectively.

The book titled ***"Law of the Press"*** by **D.D Basu,** the book adequately meets the requirements of a journalist containing the comprehensive discussion of the basic principles relating to the freedom of the Press from its constitutional, philosophical and legal standpoints. The book not as it were bargains with common themes such as the require for freedom of the Press, the protection of that freedom and the impediments thereto under the Constitution of India, within the foundation of comparable arrangements of Indian, English and American laws, but too the common law and statutory law bearing on the status and liabilities of the Press as a foundation.In this version separated from developments and issues within the beginning law on privacy, other critical themes have been managed with, counting 'trial by media', 'paidnews', contempt of court, government secrecy and protection of journalistic sources.

The book titled ***"Constitutional law of India"*** by **J.N Pandey**, this book has been brought up to date by incorporating all constitutional developments and judicial decisions relating to the several aspects of the privacy protection in India.

The book titled ***"Constitutional Law of India"*** by **K.C Joshi**, he was attemptedto express complicated ideas with clarity and accuracy. His work incorporates all the important judgments of the Apex Court and the High Court related to privacy law in India.

The book titled "***Winfield & Jolowicz – Tort"*** by **W. V. H. Rogers**, is a significant help to understand the researcher common law foundation of privacy and its relationship with defamation and other matters. The author emphasises on the protection for interest of privacy in England for which he considers the legislative provision of the Human Rights Act, 1988 and the Data Protection Act, 1988.

The book titled ***"Fundamental Rights A Study of their Interrelationship"*** by **P**

Ishwara Bhat, has proved very useful for understanding the concept of privacy in common law countries.

The book titled ***"Introduction to the Constitution of India"*** by **Durga Das Basu**, is a basic handbook on the introduction of the provisions of the Constitution. Inthis book, the author defines the various constitutional provisions in a short and precisemanner. It also provides an overview of the researcher's topic within the ambit of theConstitution of India.

The book titled ***"Select Constitution of the World"*** by **M. V. Pylee**, is an authoritative book on the constitution. This book contains a classic thought around theconstitutions of a few nations of the world. The book gets to be an awesome offer assistance to the researcher in planning the chapter on a comparative consider on the constitutional idea of the right to privacy prevailed under diverse nations within the thesis.

The book titled ***"Handbook on the Right to Information Act"*** by **P. K. Das**, is a comprehensive book about the practice of the right to information in conformity with the realistic development and participative democratic form of governance. The author endeavours to form full scope of the subject for which worldwide issues of nations like, Europe, Africa, America have been talked about within the book. The author examined the right to Information Act, 2005 within the light of other Codes, Acts, Rules, Regulations, and Guidelines.

The article titled "***Right to Privacy is the only Constitutional right when it was first advocated"*** by **Justice Louis d. Brandeis** and he co-wrote a landmark Harvard Law Review article titled '***The Right to Privacy***," with **Samuel Warren**. Instantaneous photographs and newspaper enterprise, they wrote, "Have invaded the sacred precinct of private and domestic life." It would not be wrong to state that this article stood as the bedrock of the future right to privacy justifying establishing recognizing it in International as well as Municipal legislation."

The Article titled ***"Right to Privacy": in the Perspective of the Information technology Act, 2000*** by **Dhrismitha Goswami**, presents the views about the balancing between Information Technology and Cryptography, pornography.

The Article titled ***"Right to Information vis-à-vis Privacy Right"*** **by Dr. Aparna**

Singh, another great quoting article on privacy which has been helpful in understanding 'Privacy and RTI: Balancing interests'.

The Article titled ***"White Paper on Privacy Protection in India"*** by **Vakul Sharma,** worth quoting the article on privacy which has been helpful in understandingprivacy.

The Article titled ***"Media and Law",*** by **G.N. Ray,** the President of Press Council of India, presents the views about the balancing between independence of judiciary and freedom of the press.

The Article titled ***"Right to Privacy of parties in Matrimonial Disputes"*** by **Dr.S.Srinivas Reddy**, one of the best article to analysis the privacy disputes on matrimonial life.

The Article titled ***"Right to Privacy: From Supreme Court Perspective"*** by **K.Ramakath Reddy**, this article help to understand what is UIC (Unique Identity Card) and what are the advantages and disadvantages of Aadhaar Card.

The Article titled ***"The right to Privacy in India – A study"*** by **Manasvini Krishna,** it gives the way what are the Historical development of the Law of Privacy.

The Article titled ***"The Right to Privacy in the Age of Information and Communication"*** by **Madhavi Diwan**, has been of much help to understand privacy in the modern age of technology and advance of media.

The Article titled "***Right to Privacy***" by **B.Sridevi**, this article belongs right tomedical privacy it's very helpful to understand what medical privacy is and what is thereal fact of medical privacy.

1.2 Statement of Research Problem

The concept of personal privacy isn't simple to capture in words or manner. It is known that privacy as a viewpoint of life is completely basic; one cannot do without privacyor one's 'space', Privacy is, hence, a greatly valuable and important perspective of one's identity. The journey for privacy is a characteristic moment of all human beings. As a matter of truth, it is common to require of an individual to set up person boundaries with nearly culminate disconnection. The concept of privacy in its wide clear covers a number of prospects like non-disclosure of data, sexual affairs, business privileged

insights and non- recognition by others. It may be said that the privacy is a direct opposite of being open, in the event that any private letters to one's companion are distributed by anybody without his express or inferred consent at that point his privacy would come to be violated. Additionally, in case one's neighbor peeps into his house from exterior at that point it would moreover constitute an infringement of his right to privacy. The development of the proper to protection more often than not begins from the Warren and Brandies see published within the title of the right to privacy in 1890, the learned attorney laid down that, "the right to life has come to cruel the right to enjoy life the right to be let alone; the right to liberty secures the work out of broad civil privileges". This advancement of law was inescapable. The seriously mental and passionate life and the increasing of sensations which came with the headway of civilization made it clear to men that as it were a portion of the torment, delight, and benefit of life lay in physical things, thought, feelings and sensations requested lawful acknowledgment, and the wonderful capacity for development which characterizes the common law, empowered the judges to bear the essential protection, without the intervention of the council.

1.3 Research Problems

1. What is right to privacy with a special emphasis on privacy in cyber age?
2. Right to Privacy Online – How Much Real, How Much Illusive?
3. Scrutinize the origin and development of the right to privacy.
4. Does constitutional protection of right to privacy include privacy in cyber age?
5. Does the right to freedom of speech and expression violate the right to privacy?
6. Whether electronic surveillance is a violation of right to privacy in cyber age?

1.4 Objectives of the Study

This research has been conducted with a view so as to provide a clear picture over right to privacy in cyberspace. This research work will entail the study of the **Personal Privacy in cyberspace** as an imperative right for individuals and for the community in general. The author will intend to firstly delineate to a layman what the right to privacy means, how it is different from other rights, and then how Privacy is cyberspace can be enjoyed, Is right to Privacy Online is real or just Illusive. The study is mainly based upon special emphasis on the privacy extended in cyber age. The scope research

demands the brief observation of the laws in different nation in comparison with India. Also, the researcher will try to examine the boundary that divides the Right to Freedom of Speech and Expression online and the Right to Privacy on Internet and how striking a balance between the two can help enhance human rights in general.
It is now important to critically analyze, compile and create an understanding of what exactly is Right to Privacy in Cyberspace. In the research there has been a complete and detailed discussion about all the facets of the Right to Privacy vis-à-vis Cyberspace.

1.5 Hypothesis

Privacy is a condition that is much easier to violate, and thus, is much more difficult to establish and protect. The following hypothesis have also been formulated to reach to the conclusion & Suggestions:

- It is suggested that as digital surveillance technologies advances and become more pervasive in cyberspace, individuals experience a decrease in personal privacy.
- The collection and analysis of users' online activities for the purpose of targeted advertising or content recommendation compromises individuals' privacy by exposing their preferences, behaviours, and interests without their explicit consent.
- The widespread adoption of encryption technologies contributes to an enhancement of personal privacy in cyberspace.

1.6 Research Methodology

In the examination of the Personal privacy in general and in cyber age, The Researcher has adopted the critical analyses and doctrinal approach. Research is based on authoritative texts and literature. The source for completion of this research is based on both primary and secondary sources, primary to the extent that the books will be referred, data will be collected from judgments, legislations, rules and regulations and while secondary sources such as world wide web and articles published therein are also used.

1.7 Chapterization

The researcher would like to propose following chapters in this research proposal.

Chapter -1	--	Introduction
Chapter -2	--	The Origin & Development of Right to Privacy
Chapter -3	--	Right of to Privacy under International Instruments
Chapter -4	--	Constitutional Right to Privacy in Cyber age
Chapter -5	--	Right to Privacy under Personal Law
Chapter -6	--	Digital Privacy in Indian Perspective
Chapter -7	--	Emerging Issues & Challenges of Privacy in Digital Era
Chapter -8	--	Analysis of Personal Data Protection Bill with respect to Personal Privacy
Chapter -9	--	Judicial Interpretation of Right to Privacy
Chapter -10	--	Conclusion and Suggestions

1. **Chapter One-** The Chapter Introduction is early on in nature. It briefly portrays what are the meaning, justification and impediment on right privacy. A brief discussion over concept of right and connection of it with obligation is additionally taken up to set up the claim of privacy. This chapter too depicts the sufficiency of Right to privacy. Advance the objective, statement of the problem,research methodology, hypothesis, and review of selected literature of the consider is brought forth.

2. **Chapter Second –** The chapter Origin & Development of Right to Privacy, the researcher has made an endeavour to layout the historical viewpointof the right to privacy. This chapter briefly portrays the meaning and concept of the right to privacy. As the right to privacy has been advanced through different stages from an awfully early period and consequently, the researcher examines the advancement of the concept of privacy of prior social orders under philosophical and common law establishment. The researcher moreover discussedthe different classification of privacy. The researcher encourages attempts the study of the advancement of the modern concept of the right to privacy.

3. **Chapter Third-** The Chapter Right of to Privacy under International Instruments.The Researcher outlines the global perspective of privacy law by making a comparative study of 'privacy laws in the United Kingdom, Australia, United State of America, South Africa, Canada and Germany'. The scholar lucidly madean in-depth study by comparing the provisions under the constitution and statutoryregime relating to privacy protection available in the United Kingdom, Australia,United State of America, South Africa, Canada and Germany. The research has extensively gone through several landmark judgments of American and English courts on the protection privacy in this chapter.

4. **Chapter Forth-** The Chapter Constitutional Right to Privacy in Cyber age under Indian Constitution. The scholar has discussed in detail the scope of the right to privacy within the purview of fundamental rights under the Constitution of India. This chapter encompasses the study of the right to privacy with reference to freedom of speech and expression which further exemplifies freedom of the press and modern practices of press, namely, trial by media and sting operation and their conflict with privacyinterest. The researcher has also undertaken an empirical study following the procedure of collection of data on competing interest of freedom of press and rightto privacy and the necessity of a particular law on privacy.

5. **Chapter Fifth-** The Chapter Right to Privacy under Personal Laws, lucidly discusses the available statutory and regulatory privacy protection regime and their limitations. Theresearcher analyses the Evolution and concept of Digital Privacy and anoverview of law relating to Information Technology in the International sphere. This chapter also underlines the need to fill the legislative lacunafor privacy protection. The researcher throws light into instances of gross violationof the right to privacy that has taken place during proceedings. In this chapter, the researcher has elaborately discussed on disclosureof the identity of victims as well as witnesses during a judicial proceeding.

6. **Chapter Sixth-** The Chapter Digital Privacy in Indian Perspective. The researcher analyses the Evolution and concept of Digital Privacy in Indian perspective and an overview of law relating to Information Technology in the International sphere. The researcher also explores the Countries around the world have taken steps to address privacy issues that arise from the internet, including adopting legislation implementing do not track, the right to be forgotten, breach notification and data retention policies

and how these policies and legislation are being implemented, and what the international best practices are.

7. **Chapter Seventh-** The Chapter Emerging Issues & Challenges of Privacy in Digital Era. the research investigator examines the notion of privacy, types of information that might need to be protected in cloudcomputing and the nature of the privacy challenge in cloud computing. The researcher also discusses threats to Right to Privacy through Technological meansand tools to protect the Right to Privacy and also discussed the violation of RightoPrivacy in the era of Covid- 19.

8. **Chapter Eighth-** The Chapter Analysis of Personal Data Protection Bill with respect to Personal Privacy. Theresearcher analyses the Evolution and concept of Personal Data Protection Bill and anoverview of law relating to Information Technology in the Indian sphere.

9. **Chapter Ninth-** The Chapter Judiciary and Right to Privacy. The researcher examined the tying down part of the Indian judiciary setting up the claim of privacy. The researcher went through as well as the most recent legal proclamation within the protection of the right to privacy under strongly circumstances conjointly examined adjusting privacy interface against open interface as observed by the judiciary.

10. **Chapter Tenth-** The Chapter Conclusion and Suggestions. The researcher put forth on by and large conclusion on the research topic and draws the discoveries of past chapters. The chapter ends with a few suggestive measures on protection,advancement, and awareness of the Personal privacy in Cyberspaces.

Chapter-2

The Origin & Development of Right to Privacy

This Chapter of the thesis explains and analyses meaning, scope and nature of privacy and seeks to explore its legal protection under the current legal regime in the form of "right to privacy". It further traces the origin of right to privacy under the English and Indian legal system. It examines the role of common law in the protection of "right to privacy". It also seeks to examine the role of Indian judiciary in recognition and enforcement of "right to privacy" as facet of right to life under the Article 21 of the Constitution of India.

Meaning:

Privacy cannot only be allowed to anybody, but it is an absolute precondition[23].The baffling question about privacy is, what is right to privacy. In respect of secrecy and concealment in ritual rites, all civilizations are concerned for private places. Although the idea of privacy has long been known to constitute historic dichotomies between public and private sectors, it remains unclear and is inaccessible analytically. More fundamentally today, with the introduction of invasive technology, as well as social networking and overall omnipresence of data sharing, this separation is becoming increasingly impossible to preserve. Privacy is a human right that is fundamental. It safeguards human dignity and the right of association as well as freedom of expression. It has become one of contemporary day's most critical human rights[23].

Data protection is a notion that can't be determined in an objective standard. The idea of privacy amid a hurricane is immediately described as Haystack[24]. The legislation of privacy is still more unorganized now in the booming digital era as fresh controversies continue to emerge.

[23]Available at http://www.brainyquote.com/quotes/keywords/privacy.d31j2Cey6YoXH0ml.99
[23]https://shodhganga.inflibnet.ac.in/bitstream/10603/58938/11/11_chapter%206.pdf
[24] Richard C. Ausness. The Right of Publicity: A "Haystack in a Hurricane", 1982 (978, 977-1055)

The way, in which it was designed, its scope and limitations were all subject to discrepancy, related notions of privacy, secretiveness and confidentiality led, interalia, to disagreements about its content and the question arose whether it is made up or can be assumed by an independent element in the existing legal rights. Individuals have the right to their own privacy, as participants in a different context: as citizens, as consumers in society (real or virtual), etc. The word was laid down as "consistent" and "lacquered" in terms of clarity, therefore preventing the definition and protection of privately owned rights to be of actual use. Some even claim that the effort in defining is ultimately useless. It's wrong search[25].

In 1890, when Samuel Warren and Louis Brandeis wrote an essay on law in 1890, the legal notion of privacy came forth.[26] Warren and Brande's early conception of privacy as a right to be noticed in their writings. This legal idea has been developed muddled from its beginnings. The definition above was criticized for its excessive width, even if the wording was clearly relevant.

Another important wording in the concept of privacy is that individuals, groups or institutions claim to decide when and to what degree information is sent to others about it.[27] But even this limits privacy to informational control[28].

One effective way to ease the definition difficulty is to divide the descriptive content of the right to privacy from its normative content, specifying the restrictions on security, which the latter really does and advocating what is to be safeguarded as a private matter (this should be done)[29].

Another suggestion was to distinguish reductionists from antireductionists. In formulating power, the reductionist method includes the development and implementation of a specific or narrow account that obviously implies a loss of privacy,

[25] Raymond Wacks, The poverty of Privacy, 96 LQ Rev 73, 76-77 (1980).

[26] Samuel D warren and Louis D Brandies, Right to Privacy, 4 HARV L. REV. 193 205 (1890).

[27] ALAN WESTIN, PRIVACY & FREEDOM 7 (1967).

[28] Louis Lusky, Invasion of Privacy. A clarification of Concepts, 72 COLUM. L. REV 693, 709 (1972).

[29] Judith Warren De Cew, Privacy, http://plato.stanferd. Edu./entries/privacy. Visited on 20th of November 2022.

whereas the anti-reductionist approach refers to the adoption of a larger strategy, taking the privacy claim into consideration more widely [30] . The idea is that the earlier approach to privacy will solve the problem of terminology ambiguity and make it possible for the right to be operation alised in law. The pragmatic practice of categorizing actions that are perceived as damaging to privacy interests was another very important step towards building a coherent and legally enforceable data protection account.[31]

Now, the right to confidentiality is recognized by the Court as another chapter in the law. The problem is described when the right cannot be described definitely.
The right to privacy is portrayed by Samuel Warren & Louis Brandies as an existent common law, which embodies protection of the "inviolate individuality" of the individual.

The right to confidentiality meant that everyone has the freedom to disclose or not to disclose information with others concerning their “privacy, activities, habits and relationships.” Warren and Brandies are not complete definitions of privacy and are not ambiguous, as the definition comes on the idea that privacy is freedom from publicity.[31]

James Fitzjames Stephen in his discussion in Liberty, Equality, Fraternity, regarded privacy as a matter of close and sensitive living relationships, something which the individual himself, or other people, public opinion and the law should respect.[32]
Younger Committee[33] -The relevant section of the committee's report is: our duty may be to agree on the privacy and say what we mean. It may appear a requirement of our job.

Intrusion into an issue in which the other person has valid expectations of privacy is infringing on both physically and otherwise. Data protection as generally dealt with

[30] Madison powers, A cognitive Access Definition of Privacy, 15 LAW AND PHILOSOPHY 369 (1966) Daniel J. So love, Conceptualizing Privacy, 90 CAL.L.REV, 1087, 1130 (2002)

[31] Ferdinand David Schoeman, Philosophical Dimensions of Privacy : An Anthology, 398 (Cambridge, University Press : 1st edn. 2008).

[32] J.F. Stephen, Liberty, Equality, Fraternity, R.J. White (ed) (Cambridge Cup. 1967), 160. First edition clondon, smith, Elder & Co., 1873

[33] Report of the committee on privacy. July, (1972) Cmnd. 5012.

comprises a wide range of personal, information or corporate privacy. Personal information is information which may be used for the purpose of identifying, contacting or locating an individual on its own with other individuals or identifying an individual. The privacy of information in other information is not personal with that person, his political religious ideas, and so on. The information relating to a person's employment, finance, and the like is organization's privacy.

Privacy as a notion has no gaps, redress for privacy violations was offered simply for the sake of equality from the very first days (that too under the guise of actions under common law). While attempts were made to remedy invasions of privacy, legal measures to be taken were never tampered with. Dean Prosser tried to classify several kinds of privacy infringement. [34] The categorization may be based on which to identify the legal action under the common law. Based on the categorization, the Restatement (Second) of Torts account was included.[35]

The classification made is hereunder -

1- Intrusion upon physical solitude - Physical loneliness or isolation involves land transgression, unlawful searching, and other unethical prayer for a private matter[39].

2- Public disclosure of private facts - Private disclosure involves information about a person who, though factual, is humiliating or very personal.[36] (X-rays of woman's pelvic region)

3- False light in the public eye - False information or impressions of an individual are given misleading light privacy measures, but such misleading feelings must not be defamatory and unpleasant towards an individual who has normal sensitivities. As a result, diffamation and misleading light have been overlapped.

[34] Neil M. Richards and Damiel J. Solove, "Prosser in Privacy Law : A mixed legacy" (2010).

[35] W. PROSSER HAND BOOK ON THE LAW OF TORTS : 117, at 802 (4th ed. 1971).

[39]Zacchiniv Scripps - Howard Broadcarting Co, 433 u.s. 562 (1977).

[36] Banks V King Features Syndicate 30 F supp. 352 (S.D.N.Y., 1939).

4- Appropriation of name or likeness - The use of an undesirable name, image or image of an individual's name is part of a name or likeness. A typical example of the claimant's advertising photograph.[37]

The above-mentioned categorization, however, does not include any potential violations if it is viewed in the context of cyberspace. Its breadth is broad enough to even cover violations of current privacy. In view of the aforementioned, the right to privacy may be defined as a cluster of rights, comprising the freedom to act with no restrictions and the freedom to disclose or not to disclose information.

Confidentiality, if well defined, is a psychological security condition characterized by the control of the reflection of one's self in the thoughts of others.

Whereas protection of the right to privacy is necessary in the wider public interest, the law is not excessively attentive to these concerns. It is also maintained. Any law mandating a right to privacy should acknowledge such right, with reasonable limits, not as an absolute right. We should remember that while it is vital to safeguard the right to life and freedom as individuals and to safeguard all aspects of it, it is also vital to reconcile it with the government's responsibility to safeguard society in general. It is strengthened by the quote you can have security and not have privacy, but you cannot have privacy without security.[38]

Privacy supporters are also allowed to argue that the absence of privacy protection would have harmful effects on the protection of people' rights. It is dubious that failing to provide adequate and appropriately stated privacy protection to people affects other non-negotiable rights. All of them infringe the right to freedom of expression, conscience and assembly, association, movement and other expressive acts. Legal citizens with an interest in general privacy must use isolation and self-censorship as a means to protect private and personal locations.

[37] Selsman V Universal Photo Books. ISI 18 A.D.zd 1st, 238 N.Y.S. 2d 686 (1963).

[38] Tim Mather subra K crishaswamy, et, et, cloud security and Privacy. An Enterprise Perspective on Risks and Compliance, 144 (2009).

Jurisprudential Basis of Right to Privacy

The call for recognition of privacy rights has its Philosophical and jurisprudential basis. Privacy should and should be accepted as intuitive even in the lack of a fully evident or clear philosophical rationale[39]. A privacy right has also been recognized as an aspect which governs fundamental human contact and relationships, even in the absence of extreme instances when private space or information interferes. Although a sense of personal privacy in its own particularity is subjective, in modern society, examples have become established of its common and general acknowledgement, such as secret democratic elections and free arbitrary research and confiscation.[40].

While not specifically articulated or addressed in theoretical law, privacy interests may be identified and justified in philosophical and judicial factors. John Stuart Mill supported the concept of a protected private realm in his ardent case for excluding political authorities from specific sectors which could only be subject to informal auto control.

The worth of the phrase is therefore far higher than ancillary allies and that data protection may be regarded as a legal notion of inherent worth, which is irreducible to any supposed larger interest. Based on the aforementioned, we believe that data protection is a discrete, state protection competent and demanding right.

Theories of Privacy

Historical research of privacy interpretations will highlight privacy and freedom inequalities. Although Privacy has long been recognized, the right to fit into or adapt certain areas of human existence is still denied enough attention. Each component of human existence should be protected if viewed in a liberal way. For example, if a person has a lenco derma in a bus, a white patch, on a skin, is he allowed staring at him? Is

[39] Charles Fried, Privacy, 77 YALE L.J. 475 (1968).

[40] Alan P. Bates, Privacy - A Useful Concept, 42 SOCIAL FORCES 429 (1964).

there an infringement of this woman's right to secrecy if a young lady goes by bus and another seats opposite him and glances at him for a while? The man would be guilty of stalking if he continues in nature. It would presumably be dubbed cyber stalking if the same is extended on a digital platform. If privacy is the right to share, if privacy is the preservation of an individual's inviable individuality, then all of these are infringements of private. If privacy is taken to be the right to be free, none of them is infringed. The examples raise difficulties since they are incapable of categorically defining it. In view of the ideas of privacy stated, it is therefore important to comprehend the right to privacy. Due to uncertainties in privacy legislation, is "mal behavior" in breach of the right to private, cannot the following questions be addressed in particular terms? Shouldn't a person do what privacy means? Could privacy rights to 'right to be let alone' be defined?

Data protection for individual autonomy is the first theory. It supports the premise that the right to privacy stems from individualism, that individual interest is (such as) ethically fundamental and that all values, rights and obligations stem from the person.

Black Mun's individualism

A case-law study into individualism has shown the inclination to limit groups and organizations to just collecting individuals who are interested. It is evaluated with relation to the fight between the individual and the State on all issues, be it constitutional or political. In relation to the clash between this person and the state, individualism of Blackmun outlines the history of the right for privacy. Thus, Blackmun does in actual fact contend with the freedom of the person rather than the inherent value or value of a certain kind of association in circumstances of privacy that appear to preserve a particular type of connection (marriage, religion, family)[41].

Sartrean Existentialism

The practice of considering the preservation of privacy as the defence of individual autonomy is supported by the interpretation of Sartre's existentialism, which people

[41] Moore V East Cleveland, 431, us, 494, 500 – 06 (1977) Blackmun J, dissenting.

construct and define by their choices and actions. In other words, man, whether it is God or Nature, is not restricted or defined by any bid or higher authority. This approach is combined with John Stuart Mill's interpretation of freedom theory, that considers state power to be confined to preventing harm to people and property of others by limiting the state's capacity to legislate on the basis of moral principles.[42].

According to the second approach, the substantive due process of law is restricted to the extent of legitimate interests of government. Thirdly, the protection of privacy from government intervention is considered a traditional family.

Nature of right to Privacy

Many are entitled to a more fundamental right to establish that certain more fundamental rights can only be ensured when the right to privacy is maintained. More often, one of the fundamental rights of males is the right to privacy. There is the argument here that either something fundamentally important is to be found in terms of privacy and its pleasure so that a person has the right to privacy, or they cannot be whole person unless a person enjoys privacy, so that privacy in this sense is like freedom. But these claims lack empirical and metaphysical support, which is due to the fact that privacy has to do with the security, achievement, enjoyment of other goods or respect for others, more basic rights and therefore the right to privacy, when respect for the privacy of others is ethically mandatory.

Area and scope of Privacy and right to privacy

Only a simulated definition can create a clear, well-defined notion and its scope. However, ideas separate from privacy that have been conflated with privacy may be distinguished and hence the essential ideas of privacy and privacy may more clearly be explained. Newly, trying to describe privacy in diverse fields is significant.

Now if you consider the issue critically, you should be alone. If you are alone, the

[42] David M. SMOLIN, "The jurisprudence of Privacy in a splintered Supreme Court", 75 Marq, L. Rev, 1992.

privacy of yourself would appear protected. Is that true? It depends of course on what is meant by letting go. If a person spies others innocently via his activities, he has left them alone in an essential sense, but has violated their privacy. On the contrary, if one is stuck on a lonely hill and nobody distracts himself from his destiny, it's not obvious that he enjoys seclusion. He's let alone, however. In general, but not necessarily, privacy is to appreciate isolation or loneliness. However, they're obviously different. Privacy may be enjoyed and desired.

Being harmed, suffering from a loss of pleasure and other items does not include loss of personal privacy, unless you are aware of something that damages your private. Only when evils reach the personal realm will privacy be lost. It does not invade an unwelcome odour, noise, etc., but an undesirable odour, noise, and annoyance entering a private home that does this to your own personal domain.

Freedom is frequently connected with being alone. It is usually explained that the negative concept of freedom is free from interference, not to mention. However, privacy, negative freedom, left alone, are obviously separate. More fundamentally, to force someone to do something they do not want to do is not to leave them alone, but rather to invade their freedom and not their privacy. The conceptual distinction between privacy and freedom may readily be established. The private of their fellow students can be invaded without affecting their freedom.

Many others, like Warren and Brandeis, support this position when they state that a person's right to privacy is the right to liberate him from unwelcome or unjustified disclosure of public concerns.

R.B. define privacy by saying that privacy is control over when and through whom different portions of us are perceived by others.[43].

Besides individuals today have openly acknowledged immense advances into their protection. Their knowledge and other mind and clinical trials for their young have been recognised, their children have been tested, where the data is now available in banks of

[43] R.B. Parker, 'A Definition of Privacy; Rutgers Law Review 27, No 1 (summer 1974), 275-296.

information; they recognise surveys by schools, colleges, managers, banks, credits, and many others, without any dissension at all. Plainly, there are significant troubles then in the method of clarifying security as far as specific exposure. The connections among assent and misfortunes and intrusions of protection are diverse and complex. Worry for protection may direct the making of conditions which free them from choosing whether they will surrender protection to get some ideal products.

This sort of considering protection as far as particular revelation has additionally prompted the idea that security comprises without exposure about one's individual, one's issues, and such. Unquestionably worry with protection are worry with and about undesirable exposure. This is in any case just the specific sense of exposure as receptivity to another person. Losing one's safety means going public about part of the facts in the sense that at least one person becomes aware of it. The sensation of publicity of the data does not have to entail exposure. In any case, unmistakably, anybody worried about protection should be careful about exposure, as the more particular sorts of data are plugged, the more prominent is the deficiency of security.

Privacy as Complete full access

Privacy means a person (or another legal body) having complete access to his own territory. The right to confidentiality allows you to prohibit others from (a) monitoring, (b) using it, (c) invading your private domain.[44] Privacy in the exclusive right to dispose of access to one's proper (private) domain.

That privacy is best understood as a right to ownership, and that the right to privacy is a right to enter the (private) domain. However, J.J. Thomson claims that in many situations rights that are derived from or equivalent to property rights, but are not, in fact, sui generis private rights, are so-called privacy rights[45].

This is a typical difficulty since the privacy of selective disclosure is a separate position. The accent on access as an area of transparency is correct, and crucial in this narrative.

[44] E van den Haag 'On Privacy', Nomos XIII (1971), 149

[45] J.J. Thomson, "The Right to Privacy; Philosophy and Public Affairs 4, No. 4 (Summer 1975), 295-314.

In this perspective, what is accurate and significant is that it stresses access to information as a district. Both seem to be privacy-related. If you are unable to divulge, access to them is an invasion of privacy according to your intentions. The requirements of privacy are that access to them is only controlled by that individual. It is not necessarily his privacy to respect the right of exclusive access via the purchase and therefore to gain an individual's agreement to access his private sphere. Likewise, although somebody buys the privilege of private access, scandalous media and readers show little respect for the privacy of people whose confessions they buy.

Privacy and secrecy

Privacy and confidentiality are evident so that secrecy does not necessarily mean that privacy must be respected, that secretiveness must not be revealed and privacy invaded. Furthermore, secrecy might be connected to matters not related to privacy. It is coercive not to intrude privacy to compel something to disclose. In the same way, respect for every hidden knowledge of man may be conceivable, but still showing little or no respect for his private, a person who only has coercive knowledge to compel him to disclose that information is not his private.

Privacy, as respect for persons

This shows the area of privacy, its implications and its profound connection with other values. The right to privacy is founded on the right to respect, love and friendship of worth and possibilities, which are founded on the morality of respect for individuals.

Academics, on the one hand love and knowledge of it, via the practical sciences on the one hand, complicate and difficult to disassembly a relation, which thus depends on the freedom to private and the worth and possibilities of love and friendship on the other.; Love and friendship on one hand and the knowledge about them through practical sciences on the other hand makes relationship complex and difficult to untie.

Privacy as respect for personal autonomy

The respect for privacy, autonomy and autonomy must be connected with privacy.

Many infringements of the right to confidentiality are a violation of the necessity to respect self-government. Lastly, the absence of autonomy should not, however, be included. In your words, write an example. Girls therefore have no lack of respect for autonomy in the event of hidden surveillance which the victim has never found.

A protection attack, particularly with regard to specific human feelings. In this way it is proposed that security identifies with that which, when known or disclosed, shocks an individual of normal sensibilities or causes him mental misery, disgrace or embarrassment. This methodology enjoys the upper hand over others of clarifying security such that observes the social relativity in regard of what is viewed as a question of protection. Subsequently, as indicated by one's general public and the time of society matters identifying with sexual direct, eating, drinking, family line, young lady, etc, could possibly be matters of protection. one's practices could possibly be matters of protection. In our general public, much that of fifty years prior was viewed as an issue of protection social foundation, compensation, assets, conjugal state whenever separated, nature of sickness, different sexual issue, realities about family members are not presently so respected. Since offenses against conventionality are socially relative, and this since they are characterized as far as acts which stir sensation of humiliation, hoax, trouble, resentment. The data show that any safety record, to be acceptable, ought to provide a pleasant clarification of the relativity of beliefs regarding the scope of protection but this cannot make protection essential. Subsequently, any record of security and what comprises misfortunes and attack of protection, should clarify life under extremist systems, and life in establishments, the police, the military and so forth, as existence with little security.

The privacy of ordinary sensitivities becomes general information and handles them with in sincerity, to the deepest detail of their life and thoughts so that only those who are super sensitive are attracted, injured, degraded or humiliated.

Loss of privacy

One such criticism is that numerous things might induce the sentiments connected with loss of privacy, in addition to loss of privacy. Offensive and unwise behavior and reckless, dumb, cowardly public behavior might lead to that emotion as well. In

addition, people may perhaps have obsessive thoughts about their privacy and contain a lot that is not actually privacy related.

Confidentiality, the publicity of private matters with which the public has no legitimate interests lost by misuse, appropriation or exploitation of one's individuality.

Privacy does not relate as a person and as one's own self to everything and anything, but to him. P.A. Freund talks about protecting the personality interest [46].

Involving in any human interaction includes a certain loss of confidentiality and intrusions into one's own selves. The relationship of kinship, love, friendship comes ahead of privacy as part of privacy. This creates a larger self which becomes the focus of new privacy.

The only self of the person is a thoughtful, self-aware person, usually cognizant of self-identification. Obviously, his concerns, his feelings and his body are his own, not someone else. The private space is not a problem today. The issue emerges in regard of augmentations of the self-individual come to consider numerous to be of their work as expansions of themselves, and as entitled to a similar protection as they them is which come to be related to oneself. The journals, artistic creations, books, Families are likewise extensions, and with them, their assets, and in any event, anything they relate to themselves. Unmistakably, not all that supposedly is an extension of oneself is such, and henceforth, not all that is believed to be in the space of protection is actually so. The test is, is it of oneself or not of oneself? To this degree there will be some extension to form the space of the private.

A critique of the right to privacy is believed to be a lack of standard and independent content. The argument is that it is unnecessary to look for ways to codify and implement privacy rights, as they do not contain interests already not present in human rights and property rights. The attack is doubled, a lack of content specificity and an absence of content independent. Lack of specificity and uniformity of the rights content comes from the confusion in its definition. A claim of a vagueness of the phrase should not

[46] P.A. Freud, Privacy : One Concept or Many; Nomos XIII (1971) 182-198.

prejudge its recognition by the law and adjudication of its value as a right or interest which deserves protection. It is also helpful to distinguish between right, the first relating to the legal protection we can accept and the latter referring, more generally and technically, to what we consider to be private. It is apparent from this standpoint that practical legislation has to be different from privacy and must simply specify the conditions for protection of private.

It is especially remarkable that, due to a lack of an apparent or accurate definition, numerous major and virtually applicable concepts of common law appear prima facie ambiguous.

The cultural relativism is said to indicate that the public – private dichotomy and the necessity for protection against private damages – does not have an impact socio-culturally. In India, in opposition to privacy, the predominance of a "culture of trust" is described as a historical and sociological fact which is contrary to positive privacy provisions.[47]It is false to claim that in India there is no right to privacy acknowledged since there are differences between social mores or institutions as well as the result of the prevailing ethical duties. Indeed it is recognized that such variances and cultural relativity in general are indicative of the fact that each Liberal Democorecognises the need, and value, to protect individual rights and freedoms, particularly due to the proliferation of intrusive technologies that create a new and increasing risk, of damages of personal privacy,[48].

Despite the safeguard against security as socially relative and thus strange to India on chronicled certainty, it ought not to refuse institutional insurance of protection if a current requirement for it very well may be appeared to have emerged. The new concerns raised by new advancements support the contention for assurance against security hurts significantly. Expanding measure of information streaming to and being held by mediators giving information on the web, which the information never expected to uncover. Regardless of whether we were to accept that current ways to deal with

[47] SubhajitBasu, Policy Making, Technology & Privacy is India 6, INDIAN JOURNAL OF LAW AND TECHNOLOGY 65 (2010).

[48] CARL WELLMAN, THE ETHICAL IMPLICATIONS OF CULTURAL RELATIVITY, 60 JOURNAL OF PHILOSOPHY 169 (1963).

security assurance established total records, the pressing factor of innovation have delivered them rudimentary. An intelligent reaction to these progressions is guarantee security assurance which can protect security as a rule. Late enactment in the nation has, notwithstanding, neglected to accomplish this[49]. Gupta assessment of the status of IT law 2000 after 2008 and insertion , in particular to determine that online surveillance procedures in India are insufficient to protect the privacy of persons on numerous occasions, including absence of harm detection and retrieval mechanisms.

Arguments for Defence of right to privacy

Utility of respect for Privacy:

The usefulness of respect for private life is supported by useful things such as joy, happiness and self-development. The utilitarian arguments are usually more commonly articulated as reasons in favor of the legal protection of privacy and not as reasons for the existence of a moral right. It can obviously be advantageous, even if there are no matching moral rights, for the state to grant legal rights.

Plainly, attacks of security may calls incredible wrongs, and they may allow and lead on to different indecencies.

One contention here equal the utilitarian contention against foul, hostile lead, asserting that the hurt brought about by intrusions of security is itself a justification regarding and ensuring protection, and subsequently for recognizing a good and legitimate right to protection. This can't be said as an acceptable contention. In each cases the hurt endured by the 'casualty' is one which should be borne for more prominent great of freedom Furthermore, it is impossible to make this claim to recognize either a good, a legitimate right to protection until the harm is made plain not to be produced by socially determining tendencies that may be altered quickly by training and preparation, but by indescribable innate feelings.

[49] Apar gupta,balancing online privacy in india, the indian journal of law and technology 43 (2010).

The most fundamental useful reason is that privacy breaches include or lead to other malignancies. And these can limit our own satisfaction greatly. At best this is an argument in favor of the legal protection of privacy, if the violation of the private may lead to such atrocities. It does not support a moral right to confidentiality. The usefulness of freedom is also defended. Freedom for the purpose of privacy is restricted in the interests of freedom goods. Again, the usefulness of respect for privacy was promoted by non-utilitarian ideals, such as justice, honesty and respect for others.

Protection of Non-Utilitarian values

Privacy and Justice

If privacy is not protected, there will be serious injustices, and respect for justice will be crucial for individuals. This issue occurs most often, but not solely, in relation to the databases and the use made of the data held therein. Injustices arise from the abuse of accurate information, the criminal record of a person, health, job record, credit rating and its foundations, and so on. Thus deserving, honorable citizens may be ruined because of the information's contained in data banks.

It cannot be disregarded that argument. In the event that privacy is safeguarded against such events, all invasions of privacy may not have to be prohibited. Where information is obtained from a person under condition of confidentiality, that information should be confidential between those parties breach criminal offences, including punitive and/or civil damages should be committed whenever the individual suffers substantially from an infringement of secrecy. Doctors, hospitals, government institutions such as social services, taxation and education must also be included in this programme. Perhaps the biggest risk regarding the database is by storing and spreading incorrect information about individuals. The hurt is not of private damage, but of libel, defamation and hypocrisy with the resulting injustices.

Privacy as a basic need:

The requirement for protection is differently clarified as a requirement for a space of

confinement, of closeness, of safety from perception by others and such. It is asserted that the need is one which, if not fulfilled, prompts a helpless improvement as an individual and individual, and with the end goal that we will not have the option to foster the fragile touchy sentiments and relationship so crucial to our advancement as people. Then again, the perception of different social orders of how individuals have fared in penitentiaries, inhumane imprisonments, foundations, does little to help this case. Regularly here, if a need isn't met, this outcome in chronic sickness, and problems of different sorts. However absence of security appears to be not to result either in chronic sickness or in messes. In addition, it might maybe be answered that such sentiments are only convey over's from characters and characters which were created in social orders in which protection has been regarded. Further in collectives in whom the individuals have never known security, more profound human sentiments don't create. Communities are extraordinary, philosophically based social orders. It is difficult to tell what could be closed from such claimer assuming valid.

Privacy and Freedom:

In order to safeguard freedom, we have to limit freedom and that might be true in other areas in the field of privacy. If the legal protection of freedom is the case, it will extend to the legal protection of privacy. The problem here, however, is convoluted and intricate. In order to remain free, every limit in the protection of privacy must be evaluated against the loss of freedom implied in legal privacy protection and the freedom it safeguards. Under this reasoning of freedom, a blanket protection of privacy is not justifiable. Many freedoms and in particular freedoms to investigate and learn about human beings and men and to publish and share the freedom of exploration with other scholars, historians, thinkers and the world, as one has discovered, are essential freedoms which are very important in our liberal society's structure. For us too, this independence is vital. The very lives of our liberal society or our open society are challenged, in order to protect the privacy curtailed or lost by this freedom and analogous liberties.

Respect for persons dictates Privacy:

Regard for privacy seems to be governed by respect for individuals only in that individuals usually prefer to respect their private, so that in the sense that we reject such

requests, we indicate that we do not respect them without good cause. For example, if we have solid cause to violate an individual's desires if he or she hides a tumor that is presently functional but will soon become ineffective and lethal; we do not demonstrate disrespect for the privacy of a person. This shows that respect for privacy as such is not determined by respect for the preferences of people.

As valuable for its own sake:

Fundamental rights are non-fundamental rights that are related to the value, good or ultimate responsibility, deserving of moral binding force. An analysis of the idea of privacy indicates that privacy is of inherent value. In this sense, the protection of privacy is different from the lives of people, the development of oneself, the judiciary and even freedom, even if there is scope for disagreement as to what is the basis of the value of freedom. Privacy concerns something lacking. It must essentially be a negative definition. What is the fundamental value of the lack of anything? The state of mind or the existence of a person who has privacy, not privacy itself, is desirable if anything in this domain is useful. It could be with pleasure or happiness a better analogy here. In so much as a person enjoying privacy is valued in thought or existence; it will be because it comprises benefits such as pleasure or contentment.

In this way, each right of protection is subject to various rights and goods. This means that it is a dependent right rather than a right in general. Whether it's a subordinate right, subsidiary rights to life, selfadvancement, equity, moral uprightness, etc. depend on realistic considerations as to whether respect for protection is needed for enjoyment of such rights. It'll be once in a while, and it won't be included in certain situations. Along these lines any endeavor to give cover lawful security to one side to protection will be at risk for ensuring what should not to be secured and of consequently outlandishly limiting freedom, request and similarly significant, the acknowledgment of equity.
There are restrictions not just that the public interest can generate a right to privacy, but also because it is subject to qualifiers on the basis of its very premise and in conflict with other rights. It is apparent that, like in marriage, friendship and some other social ties, we might consent to forget privacy correctly by placing specific sections of our life outside the realm of private for others. Consensus can nonetheless be incorrectly

granted and wrongly accepted, as if someone compromises themselves and his personal privacy, selling his disgusting admissions incorrectly agreed in such instances and respecting many credit-worth. The problem here is complicated and cannot easily be regulated by the State, in particular through the employment of criminal legislation. Civil legislation, the establishment of advisory organizations, and the establishment of privacy rules can assist, but the correct respect of privacy ultimately must depend on the morale and the integrity of the individual.

Similarly, other important explanation is given by "Alan F. Westin. He defines privacy as the claim of individuals, groups or institutions to determine for themselves, when, how and to what extent information about them is communicated to others."[50] "Commenting on Westin's definition of privacy, Professor Louis Lusky points out that literally, it declares my privacy to be invaded, or at least affected somehow, if my one neighbour tells my second neighbour (without my consent) that I am vegetarian or that I am suffering from fever, or that I like oyster. The more troublesome aspect of the Westinian definition, according to him, is that it confuses through over simplification. So Louis Lusky redefines Westin's definition as privacy is the condition enjoyed by one who control the communication of information about himself."[51]

Arthur Miller "defines privacy as a control over information. For him, privacy is the individual's ability to control the circulation of information relating to him - a power that often is essential to maintaining social relationship and personal freedom. The definitions of privacy in terms of 'control over information about ourselves' has been criticized as being overbroad and narrow. Richard B. Parker is perhaps the only one who has addressed himself with the question as to what criteria a definition of privacy should meet. He maintains that ideally a definition of privacy should be as true(fit the data) as beautiful (simple) and as useful (applicable) as possible".[52]

By "data" he means "our shared institutions of when privacy is or is not gained or lost."

[50] Alan F. Westin, Privacy and Freedom, PP.7 (1970).

[51] Louis Lusky, Invasion of Privacy: A Clarification of Concepts, LXII Colum. L. Review, PP 693(1972).

[52] James Q. Whitman, The Two Western Cultures of Privacy: Dignity Versus Liberty, 113 Yale L.J., PP. 11 51 and 1181 (2004).

It may be that our shared concept of privacy may not have common characteristics. Thus the simplest definition may have to include a list. A third criterion which a definition of privacy should meet is applicability by lawyers and courts.[53]

In the light of the above premises Richard B. Parker gives his own definition in the following words:

"Privacy is control over when and by whom the various parts ofus can be sensed by others."[54]

These definitions emphasize on communication of circulation of private information. For them if there is no communication or disclosure of information that cannot amount to invasion of privacy. For this reason, these definitions are inadequate because there may be invasion of privacy without having communication to others also.

For example, "in certain situations, when a private 'eye' a photographer tracks an individual, that person's privacy may be invaded but in such instance there is no communication or disclosure of personal information". Many private interests that have been constitutionally recognised involve neither dissemination nor acquisition of personal information. If somebody plays music in public buses or a beggar goes from door to door, there is no communication of private information which may constitute violation of privacy. It is not covered by these definitions. There are other definitions which would be worthwhile to mention here.

"Privacy is an outcome of a person's wish to withhold from others certain knowledge as to his past and present experience and actions and his intentions for the future. The wish for privacy expresses a desire to be an enigma to others or more generally a desire to control others perception and beliefs vis-a-vis self-concealing person".[55] This definition highlights the psychological aspect of privacy.

In the "United Kingdom both the Justice Report, 1970 and the Younger Committee Report, 1972 pointed out that the difficulty of finding a precise and logical formula which could either circumscribe the meaning of the word 'privacy' or define it

[53] Jerry Kang, Information privacy in Cyberspace Transactions, 50 Stan. L. Review, PP. 1193 (1998).

[54] Robert C. Post, The Social Foundations of Privacy: Community and Self in the Common Law orts, 77Cal.L. Review ,PP. 957 (1989).

[55] Sidney M. Tourad, Some Psychological Aspects of Privacy, 31 Law and Contemporary Problems (No. 2 Spring), PP.307 (1966).

exhaustively. Each, however, suggested a working definition. Justice Report defines privacy as that area of a man's life which in any given circumstances, a reasonable man with an understanding of the legitimate needs of the community would think it wrong to invade."[56]

"Govind Mishra defines privacy as a fundamental right of the citizens to exclude governmental acts, omissions and things which tend to annoy or embarrass them and which affect the promotion and maintenance of their dignity".[57] "However, it is not an exhaustive one. He accept that privacy is a culturally limited concept".[58]

Secondly, the objectives of the arguments tend to differ. For example, Dean Prosser's famous essay, which marshalled several hundred privacy cases, was a successful attempt to demonstrate that the American law recognised four distinct torts under the umbrella of 'privacy'. In his well-known rejoinder Edward Bloustein seized upon Dean Prosser's atomisation of 'privacy' and insisted that there is a single interest at the heart of the law's protection, namely 'human dignity'. "But in exposing the disparate interests protected Prosser is merely describing the law; in his reply Bloustein whatever the merits of his argument, is engaged in seeking, at a higher level of abstraction, a wider explanation for the law's concern to protect privacy". [59]

Thirdly, "the arguments as to the desirability of 'privacy' frequently proceed from different standpoints. Some see privacy as an end itself, while others regard it as instrumental in the securing of other desirable social ends such as 'creativity', 'love' or 'emotional release'. The former position, though it is central to any argument in favour of privacy, does not adequately explain why it should prevail over competing interests such as free speech. The later position is based on unproven empirical speculation. If they are to have any force, the two arguments must be seen together rather than in opposition. Fourthly, the definitions usually beg more questions than they are designed to answer. For instance, privacy is widely defined in terms of 'control' over who has information about or access to the individual. But in order to evaluate such definitions we need to know, for instance, what purpose, if any, is served by the exercise of this control. Normally the answers point to arguments in favour of the individual's right or

[56] Justice Report (Privacy and the Law), P. 5 (1970).
[57] Govind Mishra, op. cit, p. 139.
[58] Ibid.
[59] The Younger Committee Report (Report of the Committee on Privacy) , PP.10 (1972).

claim to or interest in limiting the exposure to which he is subject, or in the circulation of facts about him. Another defect of the 'control' definition is that it fails to account for the act that if I want you to know a fact about me and I am unable to communicate it to you then, according to the definition of 'privacy' in terms of control, I should have lost privacy for I have lost control over the circulation of information about myself. Equally, if I succeed in total disclosure of any private life to you I should not have lost privacy. Neither of these can be correct".

The debate is ultimate futile for, in those legal systems which recognize a common law right to privacy (for its equivalent), privacy is entrenched in a vocabularyof the courts, where it is accorded statutory protection then privacy is simply what the legislature says it is.

Kinds of Privacy

"Absolute privacy, except for the individual living alone on an island, had never existed. In the small towns and villages where most people lived before the industrial revolution, there was little or no privacy".[60] "The details of one's wealth or health could not be hidden for long from other community members. Indeed, someone seeking privacy from the others might have been looked with suspicion. Hence, the quest for privacy is inherent in man. It is a natural need to establish individualboundaries and to restrict the entry of others into that area. There are moments inevery man's life when he does not want intrusion on privacy threatens that liberty". Therefore, the concept of privacy can be classified under the following heads:

(i) Social Privacy
(ii) Family Privacy
(iii) Individual Privacy
(iv) Legal Privacy

Social Privacy

The third type of privacy is social privacy. This privacy can further be sub-divided into two categories:

(a) Professional Privacy,

[60] Jeremy Refkin, Biosphere Politics, 154 (1992).

(b) Community Privacy

Professional Privacy

One of the areas in which privacy of an individual can get affected is that ofthe professional and through the professions. When a professional acquires knowledge of private activities of an individual, it cannot be safeguarded unless professional privacy is made possible. A professional may also have his own privacy of vocation to safeguard. Hence, in the case of professional's safeguard to privacy may become essential on two scores - Firstly is own professional privacy, and secondly, the professional privacies of his clients.

Generally, in India, lawyers, doctors, chartered accountants, consultants, document copiers, magicians, astrologers etc. are the professionals who have theopportunity to possess knowledge about the privacy of their patrons. "The above as well as other categories of professionals including businessmen may have their trade secrets, inventions, special methods of operations and so on and so forth. They assiduously strive to guard their secrets and privacy for continual success as well asfor avoiding competition. The safeguard of professional privacy therefore becomes vitally important to them because with protection to their privacy, they can hope for protection to their life and personal liberty". [61]

"A doctor revealing about the disease of his patient to his employer may result in the termination of the service of the patient rendering him without the means of his livelihood or a discreet doctor having carried out an abortion for a maiden, can come into trouble by one leak in his professional privacy. Similarly, a lawyer or a chartered accountant can violate the privacy of his client by several means". In R. M. Malkani's case,[62] "the Coroner's attempts to extract bribe from Dr. Adatia has been a typical case of an attempt to violate professional privacy. Hence professional privacy needs to be safeguarded vehemently not only because it can affect the professional, but because it can also affect lives of individuals who seek help of the professionals. In the context of modem living, professionalism has come to stay in a long and important way and hence it would adequately need and deserve all legal safeguards. By protecting

[61] http:www.privcayinternational.org/reports/india. Visited on 10th of July, 2022.
[62] R. M. Malkani v. State of Maharashtra, AIR 1973 SC 157.

professional privacy, we will be in a position to protect right to life and personal liberty". [63]

Community Privacy

The concept of community privacy has a very limited field because a society is composed of conglomeration of communities and social laws generally govern major aspects. "But there is certain community privacy which may need intervention of law for their safeguard. A Hindu Brahmin community would not approve of a slaughter house for beef in the midst and cluster of their business and residential colony. Nor would Christians and Muslims approve of a ban on cow slaughter. For them beef eating is their privacy of food and dietary habit and they would not wish to surrender this community privacy. Similarly, every community can have some peculiar customs and rituals private to their own community, which they would not like to expose to public gaze or interference".

"Many communities hold certain beliefs and religious dogmas from which theyadopt their special ways of living. Any interference from outsider to this way of life, they are unwilling to tolerate and, therefore, they would need the right to privacy for their community collectively. Especially in Britain in the recent times there are secret organized groups of people involved with the supernatural. They are composed of interested believers, worshippers and practitioners, and they are known as Covens or witches of members of black mass cults. There are other such groups constituting membership of Voodoo priests, magicians, cabalistic, etc. They staunchly follow the beliefs, rights and rituals which are generally carried out in strict secrecy".[64] "Whether these beliefs are well founded or they are misconceived cannot be thesubject matter of any rationalist court but situations may arise when the court would becalled upon to determine the right of privacy of these secret societies or groups. In India fortified by Articles 25 and 26 coupled with Article 21, these groups can certainly claim privacy for their practices without any blanket bar on superstitions".

For instance in *Saifiidin Saheb* v. *State of Bombay*,[65] our "Supreme Court has held that the head of the Dawoodi Bohra Community has the right to excommunicate any

[63] http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2350631 . Visited on 15th of July, 2022 at 3.25 pm.

[64] Based on 'Supernatural' by Douglas Hill and Pat William (New American Library).

[65] AIR 1962 SC 853.

member of the community. The power of excommunication is vested in him forthe purpose of enforcing discipline and for keeping the denomination as an entity. The court further held that the community as a whole has a right through its religious head to manage its own affairs in matters of religion under Article 26(b) of the Constitution. The person who is excommunicated may be affected but the power of excommunication is mainly for the purpose of ensuring the preservation of the community and it is prime significance in religious life of every member of the group. This is community privacy".[66]

"But ex-communication of a member of a community affects many of his civil rights and to that extent his personal liberty is also affected. An individual cannot be treated as a pariah and he has the right to follow the dictates of his own conscience. Article 21 as it is being interpreted today was not available at the time when this case arose. Otherwise the court could have granted the right of privacy to an individual in religious matters".[67]

Even in modem sophisticated society, the members of Masonic Lodge take oath of secrecy and they jealously guard its privacy. To this extent community privacy may also become an important subject for the consideration of our juridical minds.

Family Privacy

"A concept of family privacy can cover a wide area beginning from the privacybetween a married couple, extending to a joint family living together and ending with all the blood relations of the family though they may not be living together. It is often seen that a family secret is assiduously guarded by the members of a family although they might be living in different towns. In India during the olden times people lived in joint families and it was only when our society became progressively urbanized thatthe institution of a joint family underwent changes because of changing forms of social institutions and not through the need for privacy. The social customs and the cultural background were such that the families were auto-adjusted to certain kinds of privacy and the individuals never even felt the need of intervention of law or that of any court.

[66] http://indiatoday.intoday.in/story/data-collected-for-supreme-court-centre/1/350993.html Visited on 20th of July, 2022.

[67] http://www.nyulawglobal.org/globalex/india.htm. Visited on 20th of July, 2022.

The safeguards were in built in the very customs themselves. There was segregation of males and females and unwritten social rules automatically created and granted privacy. A friend or a relative visiting the house would do so without encroaching upon the permissible limits of privacy". [68]

"It was only after the fragmentation of the joint family under the on sought of urbanization and its economic impact, that people became self-centered. In order to share selfishly the privileges of wealth and pleasurable living - not necessarily a happy and contended living that different factions in the family made the need for privacy a dominant tool for their segregation. As a result of this, plausibly the need for family privacy has assumed significance and law has been compelled to favour the clamorous demand for it and the judicial activism has become a collaborator".[69]

Legal Privacy

Under this privacy, certain intimate liberties are protected from the intrusionsof the government. "The intrusions by the government are regulated by means of law and the law in turn either gives or takes away rights to certain liberties which will have considerable bearing on privacy. The examples of regulations are:

a) Procedure of search and seizure;

b) Publications of news;

c) Eavesdropping/wire tapping;

d) Taking photographs;

e) Birth control;

f) National security. Public nudity (exposure);

g) Sexual relationship beyond marriage;

h) Privacy of court proceedings (trial in camera); and

i) Tax recovery and income.

[68] Andrew T. Kenyon, New Dimensions in Privacy Law, Cambridge University Press, PP. 2, 2007.

[69] http://indiatoday.intoday.in/story/data-collected-for-supreme-court-centre/1/350993.html Visited on 25th of July, 2022.

Since these subjects need a separate and quite an elaborate discussion the researcher has only mentioned the areas in which human society can lay claim to privacy as can be seen from the American legal literature. So long as the Indian society is not enveloped by the American evaluations and devaluations, it is not likely to make any hard demands on the Indian Constitution and Article 21 will not have to reach its elastic limits to finally break down, while bearing the burden of privacy".[70]

Individual Privacy

"The most susceptible area is the privacy of individuals. An individual by nature at some time or the other in his daily existence craves for brief periods of privacy for mental peace, quiet, meditation, enjoyment of hobbies, cultivation ofpersonality, both by cosmetically means as well as by rehearsals and practices such as speech modulation, physical exercise, etc. Thus quest for privacy is inherent in every human being. Man's pursuit of seclusion is in reality his pursuit for privacy and since privacy is an integral part of one's life the right to life cannot be complete with any abnegation of right to privacy". [71]

In our complex society as per individual idiosyncrasy the manifestation of demand for right to privacy may appear even in paradoxical forms. "Whereas on the one hand the Indian women may go for choice of apparels which expose their bodiesto the public gaze to the minimum in the American society, as we have already seen earlier, the women may want to bare their bodies to the maximum and making the right to privacy paradoxical. Any attempt on the part of the authority to forbid the exposure of their anatomy on grounds of obscenity may well be construed by these women as an infringement of their right to privacy of their bodies which they wish to exhibit publicly". Women when they do not mind exposing their anatomy in public, they are assiduous defenders of their age, which they wish to hide by all means.

"Any effort on the part of the government or the society to restrict the right to privacy of an individual who wishes to choose his own way of life, associations, profession, faith, religion and so on and so forth would definitely mean to him that his privacy is at stake. Generally governments, journalists, social scientists, employers and relatives

[70] http://www.ssrn.com/abstract=2133915. Visited on 14th November, 2022 at 8.20 pm.

[71] S. K. Sharma. Privacy Law -- A Comparative Study, Atlantic Publishers and Distributors, New Delhi, P.11 (1994).

constitute a class of intruders of individual privacy".[72]

It may thus be summed up "that the long search for a definition of 'privacy' has produced a long-lasting debate that is often sterile and ultimately futile for, inthose legal systems recognise a common law right to privacy (or its equivalent), privacy is entrenched in the vocabulary of courts, where it is accorded statutory protection then privacy is simply what the legislature says it is. The preceding study also discusses the functions of privacy as described by Alan F. Westin. It is revealed that the entire description is predicated upon a civilized social life." Professor Westin has not deliberated over the role of privacy in the transformation of a natural society to a civilized one. It is abundantly clear from the foregoing study that the conceptual basis of privacy is an original sovereignty over oneself. Privacy is the recognition of individual autonomy and inviolate personality. It seeks protection of human dignity in a clear tune. Standing and integrity of a person can be preserved out of the concept basis of privacy. It obeys the sacred relation with spouse, family and recognizes a person's home as his castle. Privacy harmonizes social and individual relation. It gives place for genuine human emotions. It does not allow commercial utilization of an individual's personality. Finally, it encircles a person's inner zone with a view to restore his status at art of his fellow member of society. Further, the contours of rightto privacy remained undefined and an attempt has been made to analyse the scope, extent and effects of this right.

[72] http://www.cia.gov/library/publications/the-world-factbook/geos/in.html. Visited on 26th of November, 2022 at 11.45 pm.

Chapter-3

Right to Privacy under International Instruments

The right to privacy is recognition of the individual's right to be let alone and tohave his personal space inviolate. "The need for privacy and its recognition as a right isa modern phenomenon. It is the product of an increasingly individualistic society in which the focus has shifted from society to the individual. In early times, the law gave remedy only for physical interference with life and property for trespass. As civilization progressed, the personal, intellectual and spiritual facets of the human personality gained recognition and the scope of the law expanded to give protection to these needs".[73]

The common law has for a century and a half protected privacy in certain cases,and to grant the further protection would be merely another application of an existing rule. It is unwarranted invasion of individual privacy which is reprehended and to be, sofar as possible, prevented.

Liberty for the individual in his private life is secured by the ordinary law of theland, enforced by the court. The common law allows the individual to speak and act in his own home as he pleases and to carry on his daily business provided that in so doinghe not infringe the rights of others or behave in such a way as is likely to cause a breachof the peace or commit an offence. The law does not include a general right to privacy but a number of provisions apply in particular circumstances to protect privacy.

Certain forms of intrusion may involve criminal offences for example, interference with the mail or with telephoning systems, the use of unlicensed radio transmitters for 'bugging', the harassing of tenants to make them quit, or the sending ofindecent or obscene matter through the post. Other attempts to obtain private information might involve offences of breaking or entering. In some instances of intrusions on privacy, the civil law of trespass, of contract and copyright, or of breach of confidence may provide a right of action leading to pecuniary damage.[74]

---

[73] Madhavi Divan, The right to privacy in the Age of information and Communications, Supreme Court Case (J) 2002 (4) pp.12-23.

[74] Dr. Juris jon Bing, Data protection , 1996 available at

In United Kingdom and other common law countries privacy right of individuals is protected by law of law of torts and a variety of statutes. "In common law some of the interests involved in privacy was protected from very ancient times. Despite the fact that interest involved in United Kingdom from ancient times, the violation of privacy rights has not so far, at least under the name, received explicit recognition as a tort by British Courts. Several reasons may be cited for this: -

i) The traditional approach was to formulate tort liability in terms of reprehensible conduct rather than specified interests entitled to protection;

ii) British Courts have been content to grope cautiously along the grooves of established concepts like nuisance and libel rather than make a bold commitment to an entirely new head of liability;

iii) It was very difficult to draw a clear line between what should and what should not be tolerated with regard to privacy interest.[75]

There is a school of thought of which is the most outstanding spokesman that privacy is not an independent value at all but a composite of interest in reputation, emotional tranquility and intangible property". The view of Dean Prosser has been adopted by Salmond. In spite of non-acceptance of privacy as a separate common law right a combination of statutes and the common law have in their own pragmatic way protected very effectively the interests included in privacy rights. "Although English common law does not recognize invasion of privacy as a tort in all cases in which the American courts do. There are four distinct which are discovered in these cases:

i) Intrusion upon a person's seclusion or solitude or into his affairs;
ii) Publicity which places an individual in false light in public eyes;
iii) Appropriation to s person's advantage of another's name or likeness.

The interests protected in these cases are interests in freedom from mental distress, in public disclosure and in false light cases, the interest in reputation and in appropriation cases, proprietary interest in name and likeness; from this angle the prized right of privacy shrinks in stature so that it becomes a mere application to novel circumstances of the traditional legal rights to protect well identified and established social values. In

http://www.jus.uio.no/iri/rettsinfo/lib/papers/dp_ norway.html. Visited on 11th of November, 2022 at 10.20am.

[75] Winfield, Privacy, Vol.47 LQR (1931), pp.135-149.

this view, privacy is not an independent legal right protecting a fundamental human value. Assaults on privacy are transmuted into a species of defamation, infliction of invasions of mental distress and misappropriation. Accordingly, there is no new tort of invasion of privacy but only a composite of the value society places on protecting mental tranquility, reputation or intangible forms of property. Whereas Warren and Brandeis thought that privacy is exclusively a remedy for a single tort, Dean prosser thinks that what is involved Is not one tort but a complexof which would seem to pertain distinctively to any interest in privacy." These interests were protected by English Courts through a wide array of established torts like trespass,nuisance, passing off and defamation.

- Trespass

  Intrusion on plaintiff's solitude and seclusion is a violation of privacy as they are the primary interests involved in privacy right. The tort of trespass furnished adequate remedy against physical intrusions into plaintiff's possession of property. Planting of listening devices in plaintiff's home or taking photograph after gaining unpermitted entry was considered as trespass. However, the tort of trespass had its ownlimitations in protecting intrusions on privacy. They were ineffective in cases where thedefendant operates outside plaintiff's possession area as in case of 'peeping toms' snooping, illegal wiretapping, use of listening and recording devices, etc. The Tort of nuisance was to a certain extent effective in such cases which fell outside the mischief of trespass.

- Nuisance

  Intrusion of a person's privacy was considered a nuisance from very early period. This tort was used to help a plaintiff whose privacy was interfered with by activities taking place outside his land.

  In *Berstein* v. *Sky view Ltd*.[76]defendant's business was to take aerial photographs of the premises from a height of several hundred meters and then offer them for sale to the owners. The plaintiff who was the owner of the country house whosephotograph was taken objected to it and demanded that all negatives and prints should be destroyed. The court observed in this case that constant surveillance through air is amonstrous invasion of privacy. Thus tort of nuisance was used to protect privacy.

[76] 479 [1978] Q.B.

- Defamation: passing off

Public disclosure of embarrassing private facts is another area of violation of privacy right. The English Courts have protected this privacy interest in several cases using tort of defamation and a very unique technique of breach of implied contract. In an early case of *Prince Albert* v. *Strange*[77] Court granted an injunction restraining defendants from reproducing lithographic copies of drawings which the royal couple had made for their children. "In *Argyll* v. *Argyll*[78] plaintiff Duchess of Argyll married to first defendant Duke of Argyll moved the court for an interlocutory application against publishers of newspaper from publishing the article of first defendant containingsecrets of plaintiff relating to her private life and private conduct. These secrets were communicated by plaintiff to first defendant in confidence. The court allowed the application and granted injunction." In all these cases courts had prevented disclosure of embarrassing private facts thus upholding right to privacy of plaintiff's.

"The term appropriation of personality denotes unauthorized use of a person's name or picture in aid of advertising of commercial purposes." Such appropriation violates the basic privacy interest of control over use of name, likeness. Courts in UnitedKingdom have provided remedy in such cases through the plastic category of defamation and passing off. The tort of passing off has contributed in protecting privacy.

Statute Protection of Right to Privacy

"The average Englishman's habits of reserve and regard for his own privacy are legendary. It is surprising, therefore, that English courts have, until very recently, shown great reluctance to recognize privacy as an interest worthy of legal protection in its own right. The experience of other common law countries has not been the same; privacy law has flourished in the United States and has gained a foothold in Australia and Canada. Moreover, a right to privacy has received international recognition Yet in England, parliament has refused on a number of occasions to enact broad privacy protections, and the courts have been slow to find a grounding for privacy in the common law and in the constitutional principles as the American courts have done. Judicial pronouncements in the past few years, however, have cone closer and closer to recognition of a general privacy interest protected at common law as one of the rights

[77] 2[1849] Q.B at pp. 652.
[78] [1965] Vol.1 All.E.R.

of every English subject."[79]

The right to privacy does not receive explicit recognition in English law. "To theextent that privacy rights exist implicitly in Britain, they are formulated quite differentlythan in the United States. Indeed, a popular treatise on privacy in Britain does not discus freedom of choice in the areas of sexuality, reproduction or familial relations. Although British law does address these issues, they do not fall within the rubric of privacy. As a result, privacy rights in Britain are a 'patchwork affair'. Early judicial decisions and legislation lacked and notion of privacy. This reflects, in part, a reservation of authority to make laws regulating any aspect of community life. Additionally, British Governments resist any legal restrictions on the exercise of their powers. Britain has also declined to adopt domestically the right of privacy guaranteed by the European Convention on Human Rights". "Although article 8^{137} guarantees British citizens a right of privacy, Britain remains the only signatory to the European Convention on Human Rights, without a law of privacy thus, under domestic law, the individual citizen have no guaranteed right to seek redress against intrusive government activity."

The English jurisprudence has tried to give effect to this right bit under one or the other existing rights. In English Courts 'right of privacy' has yet to gain recognitionas an independent existing right. However, there is a ray of hope because the jurist like Winfield has mentioned infringement or violation of privacy as a Tort though a 'doubtful Tort'. This recognition by Winfield goes on with his definition of Tort as different from the 'pigeon-hole' definition of Solmond. Even apart from the nomenclature the concept has crept in the decisions of English Courts as will be demonstrated and illustrated later on. "In 1961, thirty years after Percy Winfield had urged the courts to recognize a right to privacy, Gerald Dworkin remarked in the pages of the Modern Law Review that in default of judicial creativity, legislation was the only avenue open. The first comprehensive legislative proposal Bill, was introduced in the House of Lords in the year. It provided a remedy against publication without consent of a plaintiff's personal affairs or conduct unless the defendant established one of a number of defences, including 'reasonable public interest' in the publication."

"The next flurry of legislative interest arose in 1967, sparked by Alexander Lyon's

[79] William M Beaney, The Right to Privacy and Law, Law and Contemporary Problems, Vol. 31, No. 2, Privacy. (Spring,1966).

Right of privacy Bill establishing an action against unreasonable and serious interference with the seclusion of an individual, his family, or his property, subject again to several defences. Succeeding years saw a number of bills introduced to deal with one or another aspect of privacy invasion, all of them unsuccessful. Justice emerged with a draft bill in 1969, and with slight changes this was put forward by Brain Walden as a Right of privacy Bill in 1969. This Bill defined an inclusive 'right to privacy' and a 'right of action for infringement of privacy' subject as always to certain definite defences."[80]

Some protection to privacy is given by law in court proceedings, notably in criminal proceedings in juvenile courts, rape cases and in certain aspects of domestic proceeding. "In England the right to privacy of some convicted offenders is safeguarded by legislation under which a person is convicted of a criminal offence in general need not admit or reveal depending upon the nature or length of the sentence given. It does not apply to people who have received prison sentence of more than two and half years. Protection against attacks on a person's honour and reputation is given by the laws on libel and slander, injurious falsehood passing off."[81]

Statutory protection of privacy interests in common law has a long history. At present several statutes aiming at protecting a person from unwanted publicity exist in England. "Police and Criminal Evidence Act, 1984,[82] Interception of Communication Act, 1985,[83] Sexual Offences (Amendment) Act 1976,[84] Data Protection Act 1984[85] are some important legislation containing provisions protecting privacy in England. These Acts contain protection of diverse interests of privacy. Although the drive for explicit and comprehensive privacy legislation has failed, Parliament did enact, in a piecemeal and incidental fashion, a number of privacy protections of limited scope. Unofficial mail-opening and disclosure of the contents of telegrams have long been offences,[86] and it is possible to piece together statutory prohibitions against most methods of wire-

[80] Media: Problems and Prospects, published by National Media Centre.
[81] S.K.Sharma: Privacy law: A comparative study, Atlantic Publishers & Distributors.
[82] This Act largely governs official search and seize operations.
[83] The Act contains provisions protecting individuals from illegal tapping, under the Act a tribunal is constituted to consider complaints from persons whose telephones are intercepted.
[84] The Act contains provisions protecting individuals from illegal tapping.
[85] Under this Act it is an offence to publish names of rape victims without their consent.
[86] The Act requires companies using computerized personal data to register their operations with data protection registrar.

tapping and bugging. Many statutes, including the official secrets Act,make disclosure by civil servants of information obtained in confidence in the course of duty an offence."[87] More recently, "parliament has prohibited intrusive 'harassment' oftenants by landlords"[88] "wherein tenants' rooms were entered with a pass-key and furniture left disturbed and windows opened so that tenants should know that their privacy had been invaded. Parliament also prohibited intrusive harassment of any personby means of obscene and menacing telephone calls and unsolicited obscene publications. In the mid-1970s major statutory protections have been the Consumer Credit Act of 1974 providing individuals with access and opportunities to correct creditinformation compiled on them,"[89] "the Rehabilitation of Offender Act, imposingcriminal and civil penalties on disclosure of spent convictions"[90] and "the Sexual Offences (Amendment) Act of 1976, securing the anonymity of rape victims and defendants."[91] "In a dozen or so reported decisions, all within the last four years, English judges have explicitly invoked such a right, though without taking the final stepof creating a new legal right of action in tort. The House of Lords has made three such pronouncements. First, through the power of the courts to hold searches and seizures unlawful, the right to privacy prevents abuses of statutory powers of search by government officers."[92]

Secondly, "as a tool of statutory construction, the right forbids government officers to force their way into private homes without explicit authorization of an Act ofParliament and, further, gives judicial discretion (at least in some circumstances) to exclude evidence obtained in an unauthorized entry."[93] Thirdly, "in the context of civillitigation, the right limits a party's use of documents obtained through discovery, makingwider disclosure of such documents a contempt of court. In the Court of Appeal, the right to privacy has grounded even more restrictive constructions of statutory powers of search",[94] "as well as injunctions against the publication of information obtained in confidence,[95] and refusals by the Court itself to assist litigants in obtaining criminal

[87] See Sec 64, Post office Act 1953.
[88] See Sec.2 Official secrets Act 1911.
[89] Sec 158 Consumer Credit Act.
[90] Rehabilitation of Offenders Act 1974.
[91] Sexual Offences(Amendment) Act 1976.
[92] Inland Revenue Commissioners v Rossminster Ltd [1980] AC.
[93] Morris v Beardmore [1981] AC.
[94] R v Thornley (1980) 72 Crim App R 302.
[95] Schering Chemicals Ltd v Falkman Ltd[1982]QB Vol. I.

records by jury. The House of Lords recently held that the publication of articles detailing Naomi Campbell exiting a Narcotics Anonymous meeting (with associated photos) was actionable as a breach of confidence".

In *Campbell* v. *Mirror Group Newspapers*[96] "it was notable that the fact that Ms Campbell was a celebrity, and that the pictures were taken in a public place, did not prevent her from being successful because the information disclosed (about her health and treatment for ill health) was considered private in nature. In arriving at their decision, the judges had to consider the European Convention on Human Rights (which has been incorporated into English domestic law by statute) and balance the right to respect of private life (Article 8) with the right to freedom of expression (Article 10)".

Other legal Protection of United Kingdom

Committees in the United Kingdom have made substantial report on privacy,[97] on contempt of court, bearing inter alia, on issues of publicity and fair trial and on defamation. Over the past decade and a half private members' bills have been introduced into the United Kingdom parliament to deal with various aspects of privacy. "During the sixties, other bills introduced in the United Kingdom parliament dealt with various aspects of the matter with industrial espionage, with computer data banks, with electronic surveillance and with family generally. The comprehensive Walden Bill 1969 was inspired by the Report and proposals of a committee of justice, the United Kingdom section of the International Commission of jurists, and the Walden Bill in turn led the United Kingdom Government to appoint the Younger Committee whose substantial report on privacy appeared in 1972."

The Younger Committee whose terms of reference were to consider whether legislation was needed to give further protection to the individual citizens and to commercial and industrial interests against intrusions into privacy by private persons and organizations or by companies but the committee was not authorized to enquire intointrusions into privacy by public authorities. "The committee reported in the year 1972.In that year, the Attorney-General of the Commonwealth of the Australian states commissioned a report by Prof. W. L. Morrison of the university of Sydney, with particular reference to the question of the protection of the privacy of the individuals having regard to the increased

[96] [2004] UKHL 22.

[97] Report of the committee on privacy of 1972 popularly known as Younger Report.

means of collecting, storing, retrieving and disseminatinginformation."

"Younger Committee observed that while privacy is widely recognized as a legally defensible right in the United States, it is not established as a coherent principleof law and it has not significantly contributed to respect for privacy in everyday life, especially by the mass publicity media. It is generally agreed that, to this point, the Common Law of England and many other commonwealth Common Law Jurisdictions know no generalized right to privacy. In the parliamentary youth United Kingdom during the 1960's in Lord Mancroft's right of privacy Bill, 1961, Lord Denning said thatthe law on privacy in the United States had evolved from the English Common Law andthat in England 'the judges may well do it'. The Younger Committee commented that Great Britain has less in its law aimed specifically at the invasion of privacy than any other country whose law it had examined. Lord Denning's statement in the debate on the Mancroft's Bill was very much in character, but it is very doubtful if the Common Law of England would, at this time, recognize or announce a general right of privacy."[98]

Advancing technology has enabled the media to make even more searching intrusions into individual privacy and the reach of the television, with the assist of satellite, is formidable. The Younger Committee spoke of a growing tendency on the part of media to engage in "investigative journalism" and devoted a substantial part of its report to problems associated with the media. "The Younger Committee noted that from a wider point of view, concern for the protection of privacy has been simulated bythe growing pressures exerted by modern industrial society upon the home and daily lifeincluding such factors as the density of urban housing and the consequent difficulty of escaping from the observation of neighbors."

It is also likely that threats to privacy represented by the assembly of massive computerized data banks are potential, rather than actual. "The Younger Committee noted that the computer problem as it affects privacy in Great Britain is one of apprehensions and fears and not so far, one of facts and figures, and professor Morrison's estimate of the Australian situation was in substantial accord with this. He noted further that computer organizations displayed the greater sensitivity to the possible effects on privacy of what they wore doing, and the utmost anxiety to see that privacy was fully protected. There are seriously and deeply felt fears concerning the use

[98] Michael,James, privacy and Human rights, (UNESCO 1994).

to which such computer data banks may be put, especially in such fields as credit, medical and police records. There is certainly deep concern at the use of the battery of sophisticated devices available and constantly becoming available for surveillance and information gathering. Spectacular and widely publicized events add to the unease, the revelations of wiretapping, bugging and break-ins associated with Watergate have brought to many a new or renewal awareness of the scale and character of intrusions into individual privacy." [99]

The report of the Younger committee on privacy, published in 1972, contains the results of the committee's detailed examination of the whole question of the right ofprivacy. It contains proposal for the restatement of the law of breach of confidence, thecreation of

iv) a new criminal and civil offence of unlawful surveillance by technical devices,and
v) a new civil offence of publication of information obtained by unlawful means; and the establishment of administrative controls over certain activities involving a possible threat to privacy.

"The need for legislation to protect the privacy of personal information held in computer, and to set up machinery to ensure that all existing and future computer system in which personal information is stored are operated with appropriate safeguards was the main theme of Government proposals published in 1975 in a white paper, computers and privacy. As promised in the white paper, the Government set up a Data protection committee to advise on the powers and functions of a statutory authority which would maintain suitable safeguards of privacy and confidentiality in relation to personal information held on computers."

The Younger Committee noted that whenever unwanted is given to personal matter, there may be a conflict of interests between the need to respect the individual'sprivacy. "The younger Committee argued that it was appropriate to narrow the definition of privacy, that while there was an element of privacy in the state of being let alone, it was not synonymous with privacy. An unqualified right of this kind would be an unrealistic concept, incompatible with the concept of society, which implies willingness not to be let entirely alone and a recognition that other people may be interested and consequently concerned about us. The committee proposed a narrower definition of privacy which it

[99] Entick v. Carrington, All E.R 1774.

saw as having two main aspects: one, one's home, family andrelationships, the other, privacy of information, the right to be determined for oneself how and to what extent information about oneself is communicated to others. The committee recommended that the balancing of interests in each case should be left to the judgment of the press council."[100]

United Kingdom Press Council Guidelines

Pursuant to the recommendation of the younger committee, the press council ofUnited Kingdom. issued in 1976 the following declaration of principle on privacy, setting out the rules for guidance of editors in deciding when to publish stories about people's private lives: -

"The publication of information about the private lives or concerns of individuals without their consent is only acceptable if there is a legitimate public interestoverriding the right of privacy."

"It is responsibility of editors to ensure that inquiries into matters affecting the private life or concerns of individuals are only undertaken where in the editor's opinionat the time of legitimate public interest in such matters may arise. The right to privacy is however not involved if individuals concerned have freely and clearly consented to the pursuit of inquiries and publication."

"The public interest relied on as the justification for publication or inquiries which conflict with a claim of privacy must be legitimate and proper public interest andnot only a prurient or morbid curiosity 'of interest to the public' is not synonymous with'in the public interest'. It should be recognized that entry into public life does not disqualify an individual from his right to privacy about his private affairs, save when the circumstances relating to private life of an individual occupying a public position may be likely to affect the performance of his duties or public confidence in him or hisoffice.

Invasion of privacy by deception, eavesdropping or technological methods which are not in themselves unlawful can, however, only be justified when it is in pursuit of information which ought to be published in the public interest and there is no other reasonably practicable method of obtaining or confirming it. The council expects the obtaining of news or pictures to be carried out with sympathy and discretion. Reporters

[100] Media: Problems and Prospects, published by National Media Centre, New Delhi, 1983.

and photographers should do nothing to cause pain or humiliation to bereaved or distressed people unless it is clear that the publication of the news or pictures will serve a legitimate public interest and there is no other reasonably practicable means of obtaining the material.

Editors are responsible for the actions of those employed by their newspapers and have a duty to ensure that all concerned are aware of the importance of respective legitimate claims to personal privacy."[101]

Calcutta Committee: - In spite of these above guidelines many instances of invasion of personal privacy by tabloid press had occurred. Occasionally this leads to asevere criticism against the press. Discussion in the parliament regarding unethical practices indulged in by the press led to the formation of the committee under the chairmanship of Sir David Calcutt Q.C. in 1990. The committee emphasized that individual privacy should be considered along with freedom of speech and expression. The committee pointed out that freedom of expression was subject to a number of exceptions one of which being protecting individual privacy. The committee also proposed that following acts should be criminalized.

Entering private property, without the consent of the lawful occupant with intentto obtain personal information with a view to its publication. Placing a surveillance device on private property without the consent of the lawful occupant with intent to obtain personal information with a view to its publication; and Taking photograph or recording the voice, of an individual who is on private property, without his consent, with a view to its publication and with intent that individual shall be identifiable.

The committee also recommended the following defenses to the proposedoffences. "They are: -

(i) If the act was done for the purpose of preventing or exposing thecommission of any crime or other seriously anti-social conduct; or
(ii) for the protection of public health or safety; or

(iii)by any lawful authority.

Whether the recommendations would be carried out in their spirit is yet to be seen.

[101] Report of the committee on privacy of 1972.

Perhaps the U.K. may in future have a statutory body for regulating the press."[102]

Australia

Statute Protection of Right to Privacy

In Australia there is the Privacy Act 1988. Privacy sector provisions of the Act apply to private sector organizations with a link to Australia, "including: -

1. individuals, who collect, use or disclose personal information in the course of a business
2. Bodies corporate; and
3. Partnerships, unincorporated associations and trusts - any act or practice of a partner, committee member or trustee is attributed to the organisation.

Organisations outside Australia must comply with the provisions in some circumstances. Sending information out of Australia is also regulated. Since December 2001, 'privacy law' in Australia has been almost synonymous with the National Privacy Principles, which regulate the handling of personal information by the private sector. This perspective has tended to ignore other sources of privacy obligations, including increasing privacy regulation by state and territory governments, and the binding nature of representations that organisations make in privacy policies and statements."

Right to Privacy with Judicial Law

The Australian High Court rejected a right to privacy in 1937. "The decision in*Victoria Park Racing W Recreation Grounds Co Ltd* v. *Taylor*[103] refused relief to a racetrack owner whose races were being watched, reported and broadcast to the public from a platform on the neighboring defendant's land. Prior to this decision, Australian courts had indirectly come closer to privacy protection than their English counterparts, by providing that truthful publications could be found defamatory if they were not for the 'public benefit'. Since 1937, Australian courts have given recognition to privacy interests against peeping Toms, eavesdropper and wire tappers but most of the recent developments have been on the legislative front."[104] "In the past three years, the Australian Law Reform Commission has pressed forward with proposals for statutory

[102] Singh Siva kumar, Right to Privacy, The Academy Law review, Vol. 18, 1994, at pp. 191-230.
[103] 58 CLR 479(1937).
[104] R v. Padman, 36 FLR 347 (1979).

rights of action for invasions of privacy by publication of 'sensitive private facts' concerning the plaintiff by intrusion into or secret surveillance of a plaintiff's home, and by breach of privacy safeguards in personal information systems."[105]

"Some States have already enacted privacy protections along these lines but much will depend upon the vigor with which the Australian Law Reform Commission pursues its mission. In 1988 this situation changed somewhat when the Commonwealth Government enacted the Privacy Act 1988. The Commonwealth Privacy Act deals primarily with information privacy (i.e. the handling of personal information). The Privacy Amendment Act 1990 addresses the activities of credit reporting agencies and credit providers. The Privacy Act provides protection through regulating the handling of personal information by federal government agencies. This is done by establishing rules of conduct (Information Privacy Principles for the collection, retention, access to, correction, use and disclosure of personal information."[106]

These principles apply to Commonwealth departments and agencies. "The Act also provides protection for the use of tax file numbers and consumer credit information. Under the Act the office of Privacy Commissioner was established within the Human Rights and Equal Opportunity Commission. The Commissioner is empowered to take privacy protection measures in relation to Commonwealth departments and agencies and tax file number users. An individual alleging a breach of privacy can complain to the Privacy Commissioner, who is authorized to investigate and conciliate complaints. The Commissioner is empowered make determinations, which includes making a determination that an agency has breached an Information Privacy Principles and should pay damages to an aggrieved party."

"The Commissioner can also make a determination that the public interest in compliance with the Information Privacy Principles is outweighed by the public interest in the continuation of an act of practice that is inconsistent with the Information Privacy Principles. Such an act would not be treated as an interference with privacy. The Commissioner is similarly empowered to investigate and conciliate privacy complaints concerning misuse of tax file numbers in the public and private sectors. If conciliation is unsuccessful the Commissioner can make determinations which are enforceable in

[105] Privacy and Personal Information, Australian Law Reform Commission, 1980.
[106] Kiriby, The Computer, The Individual and The Law, Australian IJ, Vol. 443, 1981.

the Federal Court by the Commissioner or the complainant."

"The Privacy Act also extended the law of confidentiality through amending theFOI Act.[107] It is now required, where reasonably practicable, that a person whose affairsare dealt with in a document be consulted before that document is disclosed under the FOI Act. There are some additional information privacy provisions in other Commonwealth laws which relate to specific information or practices such as data matching, spent criminal convictions and the use of Medicare information. Otherprivacy issues such as video surveillance and telephone interception and physical intrusion into private spaces are not specifically covered under Commonwealth privacylegislation, although there may be remedies against intrusions upon privacy in this manner covered by other more general laws."

In the seminal Australian case regarding common law privacy rights, "*Australian Broadcasting Corporation* v. *Lenah Game Meats*,[108] the High Court refrained from recognising a separate right to privacy, but left open the possibility of a new tort of invasion of privacy."

United States of America

Confessional poets and Supreme Court justices were not alone in scrutinizing privacy. "An increasing number of Americans were worried about the powerful surveillance technologies of law enforcement; angered by the memory of Joseph McCarthy's unrestricted cross examinations in the House Un-American ActivitiesCommittee trials; and embarrassed by on-the-job personality testing in business, government, and the military. Nevertheless, the cold war political context created a paradox: despite the mushrooming of invasions on the individual citizen, privacy was frequently hailed as one of the characteristic rights of a democracy, one that defined theUnited States in opposition to the Soviet Union. Between 1958 and 1973, the Supreme Court ruled in landmark cases that protected privacy in all areas of an individual's life: the home, workplace, school, public spaces, and with regard to data collection and law enforcement. Yet, during the same period, poets like Anne Sexton, Sylvia Plath, Allen Ginsberg, Adrienne Rich, W.D. Snodgrass, John Berryman, and Robert Lowell published their most important confessional works." The confluence of these events-the

[107] Freedom of Information Act 1982.
[108] 185AL.R 1(200).

redefinition of a legally protected realm of private action by the courts and the unprecedented exposure of the private sphere in literature-throws into relief the complexity of a notion of privacy that is crucial to any definition of cold war U.S. culture.

"Louis Brandeis and Samuel Warren are credited with first formulating a right to privacy in the Harvard Law Review in 1890. However, the right they proposed was a tort, a law that would protect one citizen from invasion by another. It was not until *Olmstead* v. *U.S.*[109] that privacy became a constitutional issue, a conflict between the individual and the state. Brandeis, by then a Supreme Court justice, wrote an eloquent and much-cited defence of privacy in his dissent in the wiretapping case, but the Court was not persuaded that such a right existed until the 1960s when the surveillance technologies of the cold war society made intrusion by the state not only possible but commonplace as well. In 1958, the year prior to the publication of Life Studies, a case called *NAACP* v. *Alabama*[110] began the reversal of the Court's thirty six-year refusal to establish a right to privacy by concluding that a political organization had the right to keep its membership private. Only two years later, Justice Harlan's dissent in *Poe* v. *Ullman*[111], a case that challenged Connecticut's[112] prohibition against the use of birth control, began to articulate the rationale for protecting the home as a private 'zone,' which was accomplished in *Griswold* v. *Connecticut*[113]." In the latter case, "the Court 'found' the right to privacy in the 'penumbra; of protections created by the Fourth, Fifth, and Ninth Amendments in the Bill of Rights. Toward the end of the 1960s, the Supreme Court rapidly expanded the newfound constitutional right to privacy beyond the privileged space of the marital bedroom to the world outside the home. Responding to bureaucratic intrusiveness and abuses of state surveillance in public spaces, the Supreme Court, through such post-Griswold cases as *Terry* v. *Ohio*[114], *Katz* v. *United States*[115], and *Eisenstadt* v. *Baird*[116], transformed the right to privacy into one that adhered to the individual and was thus mobile and dependent on context. By locating privacy in the

[109] 277U.S 438(1928).
[110] 357 U.S 449(1958).
[111] 367 U.S 497(1961).
[112] 299 U.S. 319 (1937).
[113] 302 U.S. 319 (1937).
[114] 381 U.S 479(1965).
[115] 392 U.S 1(1968).
[116] 389 U.S 347(1967).

body of the citizen rather than in a protected zone, the Court had created a legal doctrine that was concerned less with the ability of the individual to withdraw from public space than with the right to self-determination and autonomy. This extension of the notion of privacy to mean individual autonomy culminated in the paradox of *Roe* v. *Wade*[117], a decision that marked the Court's greatest expansion of the right and first retraction of it. No longer an issue of the limits of an individual's private sphere of action, the public debate over privacy began to Centre on what and when a woman was permitted to choose and, less obviously, what a woman was compelled to say in order to enact that choice." That is, as legal doctrines moved away from an abstract notion of the democratic citizen to focus on gendered bodies, the cold war privacy debate was fundamentally altered. It will be discussed in detail here.

Statute Protection of Right to Privacy

The Privacy Act seeks to preserve the individual's interest in privacy while at thesame time recognizing the legitimate needs of government for information. "It reflects the belief that every individual should have a right to control to some extent what information the government may maintain concerning him and what uses may be made of that information, and deals as well with the individual's procedural due process rights attendant to government maintenance and use of information. The Act will be examined in the context of specific rights granted to individuals and the extent to which statutory exemptions, agency discretion, and weak enforcement mechanisms combine to effect a potential dilution of those rights. The Privacy Act of 1974 was designed to reduce both of the problems of poor data and poor oversight of access. It was an attempt by Congress to define individual rights in relation to stored data. One provision, for example, gave every individual the right to inspect and correct his or her records. The Act was also an attempt to limit use of information. Congress restricted agencies to collecting only the information deemed necessary, preferably from the individual concerned."

The main premise underlying the privacy Act 1974 is "that good government and efficient management requires that basic principles of privacy, confidentiality and due process must apply to all personal information programs and practices of the Federal Government and should apply to those of state and local government as well as to those of the organizations, agencies and instruments of the private sector. The Privacy Act's

[117] 410 U.S 113(1973).

general premise is that a record about an individual may not be disclosed without consent. However, the prohibition is subject to twelve exceptions. An agency may disclose records without consent:

1. to its employees with a need for the information in the performance of theirduties;
2. if required under the Freedom of Information Act;
3. for a 'routine use';
4. for census purposes;
5. for statistical research;
6. for historical purposes;
7. for a civil or criminal law enforcement activity documented by a writtenrequest;
8. for health or safety purposes;
9. to either House of Congress or its committees;
10. to the Comptroller General;
11. pursuant to a court order; and
12. to a consumer reporting agency.

The first three of these exceptions no doubt account for most disclosures withoutconsent; the intra-agency exception is not nearly as problematic as those allowing disclosure under the Freedom of Information Act and for routine uses under the Privacy Act. FOIA[118] contains a presumption of public access to government information."[119] The FOIA is seemingly at odds with the Privacy Act. Indeed, both statutes have exceptions to their general rules which recognize each other's interests.

"The Privacy Act provides that if the FOIA allows access to personal information as a matter of right, the person to whom it pertains need not consent to its release. The FOIA, on the other hand, provides an exception to release of information in personnel, medical, and law enforcement files if disclosure would rise to an unwarranted invasion of privacy."[120] "The U.S. Supreme Court has recently construed this FOIA provision to preclude the Federal Bureau of Investigation's releaseof computerized summaries of a person's criminal records even though the underlying records were public records"[121].

[118] Freedom of Information Act, Effective July 5, 1967.
[119] Moorefield v. U.S. Secret Service, 449U.S. 909(1980).
[120] Section 552 (b)(6) of Freedom of Information Act 1967.
[121] United States Department of justice v. Reporter's Committee for Freedom of the Press, 489, U.S. 749 S.Ct. 1468; 103(1989).

"The case offers some promise that data which is aboutcitizens rather than government will be properly refused when sought under FOIA by third persons. Still, access to personal information under FOIA will be allowed if the court finds no unwarranted invasion of privacy.[122] Courts have required agencies to produce mailing lists of government employees' names and addresses on this ground even though the Privacy Act expressly precludes the sale or rental of such lists."

"In short, the tension between the FOIA and the Privacy Act presents an issue with no clear resolution. Governments' data acquisition and disclosure are rapidly increasing with new technologies which challenge citizen monitoring, let alone keepingpace in regulating them. There is a serious question whether the Privacy Act has been adequately implemented by federal agencies. The Privacy Act's limitations have drawn criticism and suggestions for reform. Its shortcomings no doubt stem from the process of legislative compromise in drafting data protection laws to accommodate governmental interests of flexibility in administration and law enforcement."

"Since the Privacy Act[123] was passed, at least two generations of information technology have become available to federal agencies, offering new means to improve the effectiveness and efficiency of data collection and program management. The new technology also has the potential of undermining the goal of the Act to protect individuals by controlling information about them. In the ever more complex, technological, and bureaucratic environment of the late 1980s, the fair information principles of the Privacy Act are increasingly more important, but the Privacy Act scheme of enforcement and oversight appears to be rapidly becoming anachronistic. For instance, it may not be realistic to expect individuals to share responsibility to control information about themselves in view of the cost and time burdens entailed. Also, the number of organizations that retain personal information is large, and the intricacies of their uses and disclosures of information are such that it appears almost impossible for most individuals to monitor how information is being utilized. Moreover, the implicit assumption that each individual has a discrete interest in protecting his or her privacy and that no larger societal interest exists can be challenged."

"The Privacy Act of 1974 is a milestone. It marks recognition of the dangers inherent

[122] Department of the Air Force v. Rose, 425 U.S. 352(1976).
[123] Privacy Act of 1974.

in the unbridled collection and maintenance of information and the fundamental unfairness of denying an individual access to material relating to him. This recognition alone provides the basis for restoring a balance between rights to privacy and due process and governmental need for information. Since the scope of the exemption provisions will determine the ultimate value of the Act for many, they should be re-examined and drawn more tightly. The rationale behind each exemption should be articulated and examined with a critical and sometimes skeptical eye. Enforcement mechanisms need to be upgraded and perhaps even added. Discretionary power for agencies is manifest throughout the provisions of the Act. If the terms themselves cannot be stated more precisely, then perhaps principles of construction need to be added so that courts will not readily defer to agency determinations as much as they have in the past. Whatever its drawbacks, the Act is a beginning. Experience may show present fears to be minor irritations, while unforeseen complications may arise. If the Congress fulfils its function as watchdog, the foundation for further protection of the individual found here may be a turning point in the continuing relationship of government to the governed."

Right to Privacy with Judicial Law

a) The new Journalism
b) Surveillance and Seizure
c) Unforgettable decision of privacy

"Probably no branch of the law can show a greater development during the last century than the law of privacy. From a strict adherence to the rule that a court of equitywill not grant an injunction except where property rights are affected, courts of equity have in the last few years expressly recognized 'the right to be alone,' independently ofany property considerations. The American Courts have been more evolutionary as far as 'right of privacy' is concerned. There has been vivid, varied and distinct recognition and enforcement of this right in this Country. The Bill of Rights guarantees to each American protections which we equate with specific right of citizenship in a free society. The Privacy Act of 1974 is a major first step in a continuing effort to define the 'penumbra' of privacy which emanates from specific guarantees in the Bill of Rights and which helps to give them life and substance as recognized in *Griswold* v. *Connecticut*[124]. The Constitution creates a right to privacy which is designed to assure

[124] 381 U.S 479(1965).

that the minds and hearts of Americans remain free. The bulwark of this constitutional principle is the first amendment. The first amendment was designed to protect the sanctity of individual's private thoughts and beliefs. It protects the individual's right to free exercise of conscience, his right to assemble to petition the Government for redress of grievances, his right to associate peaceably with others of like mind in pursuit of a common goal; his right to speak freely what he believes, and his right to try to persuade others of the worth of his ideas."[125]

The U.S. Courts have developed privacy right on a constitutional basis. "Various amendments of the American Constitution like 1st, 3rd, 4th and 5th containing provisions protecting privacy interests had laid the necessary foundation for the courts in this regard. The Fourth amendment guarantees the right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures. In addition to the privacy of one's home and personal effects, the privacy of his person or bodily integrity and even his private telephone conversations are protected by the fourth amendment. The fifth amendment guarantees that an individual shall not be forced to divulge private information which might incriminate him." It also protects individual privacy by preventing unwarranted governmental interference with the individual's person, personality and property without due process of law.

These amendments mainly protect informational privacy. Moreover, "the ninth amendment which states that the enumeration in constitution of certain rights shall not be construed to deny or disparage others retained by people", has paved way for the acceptance of privacy as a constitutional right even though not expressly stated in the constitution. Thus using this amendment, the American Courts have read privacy right as included in penumbras of 1st, 3rd, 4th and 5th amendment of the constitution. The privacy right regarding decisional privacy was protected mainly using the ninth amendment. Evolution of privacy as a constitutional right in America was through cases which fell in following categories. The cases regarding privacy mainly gravitate around these areas.

The new Journalism

"The right to privacy-perhaps the most cherished right of all – is guaranteed, butmore

[125] Warren S.D and L.D. Brandies, The Right of Privacy, 4 Harvard Law Review (1890).

and more lately it is coming into conflict in the courts with the press right to reportfreely news. How much privacy does a person who is not a public figure have when hisprivacy collides with the rights of the press? The person's right to disseminate information was explicitly guaranteed in the constitution, and an individual's right to privacy has been obtained through a series of judicial rulings, each one put atop the other like so many bricks in a wall, since the beginning of the century."

The press's interest in raking up the past lives of individuals, often for no betterreason than sensationalism is one of the greatest threats to individual privacy. The damages caused to person's reputation by public disclosure of private facts can be enormous. In spite of the grave nature of press's intrusion on privacy, the American Courts have always been overcautious in dealing with such intrusions as they involvedfreedom of press. The obvious result is the inadequate protection to individual privacy against the press.

Freedom of press as a part of 1st amendment is considered a sacred right in the U.S. According to Justice Black: "Freedom to speak and write about public questions is as important to the life of our government as is the heart of human body. In fact, this privilege is the heart of our government: if the heart is weakened the result is debilitation; if it be stilled the result is death."[126]

"In the exercise of its traditional freedom, the press often discloses informationabout individuals which those individuals would rather conceal. When the information,though true, is particularly embarrassing or intimate, the person has sometimes felt sufficiently injured to sue the offending publisher even though the publisher committedno physical intrusion, fraud or larceny to get the story. The claimed legal injury in suchcases therefore consists only in having private information become public without the consent of the person whom the information concerns. When, in 1960, the late WilliamProsser sifted some 300 cases having to do with privacy, he found that enough of these suits had been successful to constitute a common law cause of actions. Prosser named the action 'the public disclosure tort' and listed it as one of four American common lawtorts which protect personal privacy."[127]

Even as Prosser identified the public disclosure tort action, he recognized that its

[126] Milk Wagon Drivers Union v. Meadowmoor Dairies, 312 U.S 287(1941).
[127] Prosser, Privacy, California Law Review, Vol. 48, (1960) at pp. 383.

existence might well interfere with the First Amendment right of the press to report on matters of legitimate public interest. In the intervening decade the definition of whatis 'of legitimate public interest' has rapidly expanded under a series of Supreme Court decisions,"[128] to the point where it is difficult to say confidently that any item of information which the press decides to publish is outside the protection of the First Amendment. "Though a First Amendment analysis does not by itself justify the enforcement of a constitutional right to privacy, it nevertheless underscores the weaknesses of existing constitutional privacy doctrine. The analysis directs attention to the one form of privacy which the law, both common and constitutional, has so far been unable to protect successfully: the non-corporeal, no quantifiable right to control of information about oneself, based on the content of the information rather than the circumstances of its escape from one's control. Furthermore, the analysis suggests how privacy in that form might be integrated into a system of constitutional rights. The focus on the importance for privacy of information qua information, without regard to whether its content is specifically sexual or not, is perhaps the distinguishing contribution to privacy analysis of the First Amendment approach. A First Amendment analysis of privacy teaches that an application of First Amendment guarantees exclusively to speakers will not adequately protect a free expression system; decision-makers must be sheltered, too. For the protection of privacy, the analysis yields a constitutional interest which cannot always be vindicated because it must compete with conflicting constitutional interests arising from the same logic. Yet it is the nature of privacy to be entangled with other social interests and values; privacy in law cannot be less entangled with and compromised by other legal goals. The First Amendment analysis of privacy makes these entanglements and compromises explicit."[129]

Surveillance and Seizure

Amendment IV (1971) "states that 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 oathor affirmation, and particularly describing the place to be searched, and the persons or things to be seized. The U.S. Constitution has been construed to confer almost unfettered

[128] Rosenbloom v. Metromedia, 403 U.S. 29(1971).
[129] Rosenbhatt v. Baer, 383 U.S. 75(1966).

power to the executive branch to investigate matters under its charge subject only to constitutional restrictions. Federal agencies are granted broad investigatory powers by statute in order to carry out their duties. Agencies are typically authorized to require records and reports, to inspect records or premises, and to subpoena witnesses and documents. In Shapiro v. United States[130], The U.S. Supreme Court has upheld such statutes against claims that they violate the individual's Fifth Amendment privilege against self-incrimination, reasoning that a report required to be kept by law must be considered to be a public document. While most agency data collection is by such required reports, law enforcement agencies have even broader powers to investigate; their most powerful tool is the search warrant. Both federal and state governments restrict data collection by certain techniques because of concern for individual privacy under the Fourth Amendment. When conducting observational surveillance, government officials engage in sustained scrutiny of one or more individuals. In doing so, agents attempt to avoid influencing the behavior of those they are scrutinizing. Indeed, a central aim of people conducting observational surveillance is to become part of the background to stand outside the subject and compile information about his activities without making him aware of the surveillance."[131]

"It is arguable that sustained scrutiny of this kind almost invariably interferes with privacy interests. At the very least, though, it is clear that observational surveillance interferes with privacy when the focus of an individual's attention is a private object or information. The term 'peeping Tom' provides a helpful way to illustrate this point. To classify someone as a 'peeping Tom' is to say that the person has engaged in sustained, non-consensual scrutiny of something viewed as intrinsically private. It doesn't matter that a peeping Tom stands in a place he is lawfully entitled to occupy." Someone isn't any less subject to condemnation if, for example, he stands in the public area of a restroom and stares through the slits of closed stalls. Rather, what is critical to such settings is that the person doing the observing has not respected what we may call the 'principle of ancillary privacy.'

"This principle holds that given conventional understandings that certain objects are private-the naked body, for example, or the contents of bedrooms-then sustained, non-

[130] 335 U.S. 1(1948).

[131] William C. Heffeman, 4th Amendment Privacy Interests, The Journal of Criminal Law and Criminology, Vol. 92.

consensual scrutiny of those objects even from a public place amounts to an interference with privacy interests. Needless to say, it is drawn out scrutiny that is condemned on such occasions. No one is called a 'peeping Tom' if, by chance, he notices-but then turns away from-a private object." [132]

"For nearly forty years between 1928 and 1967, the U.S. Supreme Court's decisions provided that electronic surveillance did not rise to a 'search and seizure' under the Fourth Amendment. However, in 1967 the Court ruled that electronic eavesdropping of a telephone conversation did amount to a 'search and seizure' and thata warrant was required for such search and seizure. Individual's claim to solitude and secrecy are major interest protected by privacy right." It is these interests that are violated during search and seizure by government agencies.

In America the 4th amendment and 5th amendment provide the necessary safeguards against arbitrary search. In the case of *Rabonwitz* v. *U.S.*[133] it was held that the aim of 4th amendment was to prevent unlawful invasion of sanctity of home and notto protect the person.

In *Olmstead* v. *U.S.*[134] the major issue was whether evidence given in court obtained by tapping a telephone line violated the protections guaranteed by the 4th and 5th amendments. "Two other issues involved in the case were: Is a telephone conversation private and beyond the would-be-intruder? And how does conversation fitinto the words of fourth amendment? The majority in this case opined that purpose of 4th amendment is to prevent the use of governmental force to search a man's house, hisperson, his papers and his effects and to prevent their seizure against his will. However,the majority was of the view that unless there has been an official search and seizure of his person or such a seizure of his papers or an actual physical invasion of his house, fourth amendment is not violated." Thus it was held that telephone tapping falls beyondthe scope of 4th amendment.

The above decision was overruled in *Katz* v. *U.S.*[135]. "When the Supreme Courtdecided this cases, some commentators viewed the case as paving the way for possibleexpansion

[132] Oxford English Dictionary 615 (1933).
[133] 339 U.S.50 (1967).
[134] 277 U.S.438 (1928).
[135] 389 U.S 347(1967).

of fourth amendment ‘protection’ against unreasonable search and seizure.” Subsequent developments in general fourth amendment jurisprudence, however, suggest that this hope has not been realized. Indeed, several recent cases have actually narrowed the scope of fourth amendment protection. Given these developments, it is once again appropriate to analyze the "reasonable expectation of privacy" standard enunciated in Katz. In holding that the fourth amendment "protects people, not place” the court in Katz indicated that the "constitutionally protected areas" or "trespass" standard applied in prior cases could no longer be controlling." Yet, if the sanctity of the home, which is the paradigm constitutionally protected area, is to continue to be recognized as a core value" of the fourth amendment, then the formulation and application of the reasonable expectation of privacy test should be modified in certain respects. To ensure that the fourth amendment has some minimum content that cannot be defined away by either the government or the courts, these modifications should giveparamount importance to the value of living one's daily life, particularly in one's own home, free from arbitrary and excessive governmental intrusion. Preserving this value entails recognizing that the fourth amendment does not simply protect expectation of privacy; rather, it protects the right to have certain expectations of privacy. In short, theminimum content of the fourth amendment is the minimum set of expectations of privacy to which people are entitled.

In Katz case the F.B.I. placed a “bug” on the outside wall of an outdoor publictelephone booth to tap telephonic conversation. “The telephone booth was constructed partly of glass and any one in it could be observed easily. FBI agents proceeding withouta search warrant, listened to Katz's end of the conversations. This evidence was admittedat trial over petitioner's objection. The government argued that because the agents had not physically intruded into the telephone booth, the FBI's activity did not constitute a search and seizure within the meaning of the fourth amendment. It also contended that a public telephone booth was not a ‘constitutionally protected area,’ the traditional formulation used to describe those areas protected by the amendment. The Supreme Court reversed katz’s conviction, holding that the fourth amendment protects people not places”. This fact was stressed by government to prove that there is no violation of privacy. However, the court rejected the claim. After this decision it is well settled that electronic surveillance and telephone tapping without compelling state interest is vocative of 4th amendment of American constitution.

In his concurring opinion, Justice Harlan interpreted this holding to mean that a

defendant will receive fourth amendment protection only if he has a "reasonable expectation of privacy." He explained the "reasonable expectation of privacy" test as follows: “there is a two-fold requirement, first that a person have exhibited an actual (subjective) expectation of privacy, and, second, that the expectation be one that society is prepared to recognize as 'reasonable.' If we analyze some cases it suggests that some situations deserve fourth amendment protection notwithstanding the absence of an actual expectation of privacy. As a matter of logic as well as policy, any test of what constitutes an unreasonable search and seizure must go further than merely recognizing the rights of individuals only when they possess actual expectations of privacy.” Such a test must recognize the more basic right to have expectations of privacy. The test must recognize that the advance notice that certain searches will be conducted is an intrusion in itself. Even though such an announcement may reduce actual expectations, it will not validate the search, since the notice itself violates the individual's right to have expectations of privacy. Several courts have decided advance-notice cases on the theory that, by having advance knowledge that a search would be conducted, the defendant implicitly consented to be searched.

“Technology allows law enforcement to monitor the movement of a person's carwith low risk of detection of surveillance with electronic tracking devices, commonly referred to as ‘beepers’. A beeper is a radio transmitter, usually battery operated, which emits periodic signals that can be picked up by a radio receiver. Beepers are concealed on a vehicle or other article so that directional finders may home on the signal to follow its movement.”

“The U.S. Supreme Court has held that in-transit monitoring of a beeper to tracethe movement of an article along public highways and to the vicinity of a private dwelling does not constitute a ‘search’ under the Fourth Amendment and therefore does not require a search warrant.”[136] “On the other hand, the Court has held that monitoring an object's presence within a private dwelling is a search requiring a warrant.”[137] “The use of polygraphs, commonly referred to as ‘lie detectors’, has long been controversial in the United States. The first devices were used in this country in the 1920's and the states have regulated their use in different ways since. In part because of perceived abuses by private employers in circumventing state laws, Congress enacted The

[136] United States v. Knotts, 460 U.S. (1983).
[137] United States v. Karo, 468 U.S. (1984).

Polygraph Act[138] prohibits pre-employment and random uses of polygraph tests in the private sector and generally allows them only in an ongoing investigation of theft of an employer's property. However, it does not prohibit federal, state, or local government use of the device and expressly exempts them from the statute's reach as employers. Drug testing is currently the most controversial of all government data collection strategies. The Supreme Court has decided two cases on the issue and has approved the federal government's testing in both. One case involved an employees' union challenge to the U.S. Customs Service program of testing urine samples of candidates for promotion to jobs involving the interdiction of drugs."[139]

"The union claimed that the tests were unreasonable searches under the Fourth Amendment. However, the Court sustained the program upon finding a significant public interest in detecting drug use in those employees. In other case, a railway workers' union challenged the Department of Transportation's breath and urine testing of employees involved in major train accidents."[140]

"The Court again rejected a claim that the tests constituted unreasonable searches and ruled that a warrant was not required due to the possibility of a loss of evidence due to delay. The two cases obviously do not resolve all the issues on drug testing. There are many state laws authorizing drug testing programs which are being challenged now. All that appears clear now is that, although there are weighty interestsurging for and against such tests, the U. S. Supreme Court has initially sided with a compelling public policy to detect drug abuse. The federal government's access to a person's records with a bank are governed by the RFPA[141] Federal agencies may obtainbank records upon the customer's consent or by subpoena or search warrant. Unless thesubpoena is issued by a grand jury or a judge in litigation to which the customer is a party, the customer must receive notice of the request for records and an opportunity tochallenge the access."[142]

Unforgettable decision of privacy

"The privacy of cherished decision is an eminently dynamic privacy concept compared to repose and sanctuary. The zone of intimate decision is an area within which the

[138] The Employee Polygraph Protection Act of 1988.
[139] National Treasury Employees Union v. Von Raab, 109 S.Ct. 1384 (1989).
[140] Skinner v. Railway Labor Executives' Association, 489 U.S. 109 S.Ct. 1402 (1989).
[141] Right to Financial Privacy Act 1978.
[142] United States v. Miller, 425 U.S. 425(1976).

personal calculus used by an individual to make fundamental decisions must be allowed to operate without the injection of disruptive factors by the state. This privacy is less 'freedom from' and more 'freedom to.' It is also the privacy that courts refer to in almost all the cases that discuss a constitutional right to privacy. The constitutional right to privacy was first articulated and most carefully developed in a series of cases that touched upon one of life's most intimate concerns, procreation." Two members of the Supreme Court first addressed the right of privacy as such in 1961 when a Connecticut pharmacist challenged the state's ban on contraceptives in *Poe* v. *Ullman*[143].Poe involved a constitutional challenge by a married couple, a married woman, and a physician to a Connecticut statute criminalizing the use of contraceptive device. A plurality of the Court dismissed the case on justifiability grounds, holding that becauseConnecticut had never commenced a prosecution under the statute, the question of its constitutionality was not ripe for adjudication. Justice John Marshall Harlan disagreed. In an uncharacteristically spirited dissent, Justice Harlan attacked the plurality's jurisdictional holding and offered his views on the merits. He claimed that the Connecticut statute was unconstitutional since it infringed the right to privacy in the home secured by the Due Process Clause of the Fourteenth Amendment. "Justice Harlan's recognition in Poe of a constitutional right to privacy presents a historical paradox. The privacy he defended was privacy in the traditional sense. The right at stake was not the right to use contraceptives but the right to be free of the surveillance that enforcement would require. If we imagine a regime of full enforcement of the law, 'wrote Douglas,' can make this law, it can enforce it. And proof of its violation necessarily involves an inquiry into the relations between man and wife. Banning the sale of contraceptives would be different from banning their use, Douglas observed. Banning the sale would restrict access to contraceptives but would not expose intimate relations to public inspection."

When Justice Harlan recognized a right to privacy in Poe, he was building on an established foundation. In 1937, in *Palko* v. *Connecticut*[144] Supreme Court held that the Fourteenth Amendment's Due Process Clause applied against the states only those rights that were "implicit in the concept of ordered liberty. Using this framework in *Wolf* v. *Colorado*[145], Justice Felix Frankfurter concluded that a right to privacy prevented

[143] 367 U.S 497(1961).
[144] 02 U.S. 319 (1937).
[145] 338 U.S. 25(1949).

arbitrary police invasion of private places by the states. This case involved a claim under the Fourteenth Amendment to the Constitution. Acting on information provided by an abortion patient, Denver police, without an arrest or search warrant, seized two daybooks from Dr. Julius A. Wolf's office. During his trial for performing abortions, the state introduced the daybooks into evidence and introduced the testimony of a number of Wolf's patients whose identity the seizure had revealed. Under Colorado law, evidence obtained by an illegal search and seizure was admissible in criminal trials if it was relevant, material, and competent." The evidence was admitted; Wolf was found guilty and sentenced to prison. Wolf appealed to the United States Supreme Court, arguing that the Fourteenth Amendment incorporated the Fourth Amendment and the exclusionary rule against the states and that Colorado had violated its provisions. Justice Frankfurter then applied the framework to the case at bar. He wrote: "The security of one's privacy against arbitrary intrusion by the police which is at the core of the Fourth Amendment is basic to a free society. It is therefore implicit in 'the concept of ordered liberty' and as such enforceable against the States through the Due Process Clause". As a result of Wolf, individuals had a right to privacy from unauthorized, "arbitrary" police invasion by state officers.

The next case explicitly to recognize the privacy of intimate decision was *Griswold* v. *Connecticut*.[146] "Griswold drew within the zone of privacy that is shieldedfrom state intervention. Griswold established the existence of a zone within which married persons are free to decide whether to use contraceptives without interference from the state. It was unclear, however, whether the autonomy recognized in Griswold was conferred only upon married couples. When Justice Doughlas wrote for the supreme court, in Griswold case that various constitutional guarantees create 'Zones of privacy' he was quite right in pointing out that the court was dealing 'with a right of privacy older than the Bill of rights'. Indeed 'Zones of privacy' can be found marked off, hinted at or grouped for in some of our eldest legal codes and in the most influential philosophical writings and traditions. In the early nineteen-sixties the state of Connecticut had the following laws on its books." "Any person who uses any drug, medical article or instrument for the purpose of preventing conception shall be fined not less than fifty dollars or imprisoned not less than sixty days nor more than one year or both fined and imprisoned. Any person who assists, abets, counsels, causes, hires or commands another

[146] 381 U.S 479(1965).

person to commit any offence may be prosecuted and punished as if he were the principle offender". "The Executive Director of the Planned Parenthood League of Connecticut (Ms. Griswold) and the Medical Director for the League at its office in New Haven were arrested, found guilty as accessories, and fined one hundred dollars. They appealed their convictions on the grounds that the anti-contraception statute was unconstitutional. The court held that the privacy right to married couple includes the right to decide for themselves what to do in privacy of their bedrooms."

Eisenstadt v. *Baird*[147] "subsequently extended the scope of the zone by recognizing that the right to make such a decision was an individual right, independentof marriage. In Eisenstadt the Court considered a Massachusetts law that made distribution of contraceptive materials a felony, except by registered physicians and pharmacists to married persons. The Court could find no rational explanation for the difference in treatment between married and unmarried persons: It is true that in Griswold the right of privacy in question inhered in the marital relationship. If the rightof privacy means anything, it is the right of the individual, married or single, to be freefrom unwarranted governmental intrusion into matters so fundamentally affecting a person as the decision whether to bear or beget a child. Eisenstadt declared that the purpose of the zone established in Griswold was to protect decision making of an intimate or fundamental nature and did not depend upon an intimate relationship such as marriage for its vitality."

Yet it was still unclear if the decision making protected was whether to use contraceptives or whether to have children. "The answer was forthcoming in *Roe* v. *Wade*[148] and its companion, *Doe* v. *Boton*.[149] the right of privacy is broad enough to encompass a woman's decision whether or not to terminate her pregnancy. The two cases held that right that could be deemed fundamental or 'implicit in the concept of ordered liberty' could be included in the zone of privacy. With this analysis, however, another important element was added to privacy doctrine. The state was to be allowed to invade the zone in order to protect compelling state interests, such as health, maintenance of medical standards, and protection of potential life. The Court concluded by establishing guidelines that indicated at what point during pregnancy the decision to

[147] 405 U.S 428(1972).
[148] 410 U.S 113(1973).
[149] 410 U.S. 179(1973).

abort was no longer solely in the hands of a woman and her physician. The constitutional right to privacy, however, is not an absolute right. It can be curtailed on the ground of compelling social interest or in the interest of basic competing right of other individuals." Thus decisional privacy right is well established as a constitutional right in U.S. subject to constitutional restraints.

"The fourth amendment protects the privacy of sanctuary in certain specific situations where very tangible material and very tangible premises are at issue. Beyondthose situations, the zone of sanctuary is an uncertain shield against the state's extractionof data for its own purposes or against publication of private facts by the press. The zoneof repose has never received any constitutional protection. Each zone protects a unique type of human transaction. Repose maintains the actor's peace; sanctuary allows an individual to keep some things private, and intimate decision grants the freedom to act in an autonomous fashion. it should be recognized that the right of privacy is a continually evolving right."

In Planned Parenthood of *Missouri* v. *Danforth*,[150] "the Court struck down a law requiring a husband's consent, or parental consent in the case of unmarried minors, as a condition for an abortion. Since the state may not prevent even minors from having abortions in the first trimester, it cannot delegate to 'a third party' such as a husband or parent the authority to do so."

The voluntarist grounds of the new privacy found explicit statement in *Carey* v. *Population Services International*[151] "case invalidating a New York law prohibiting the sale of contraceptives to minors under age of sixteen. For the first time, the Court used the language of autonomy to describe the interest privacy protects, and argued openly for the shift from the old privacy to the new."

Canada

Statute Protection of Right to Privacy

"Canadian privacy law is governed federally by multiple acts, including the Canadian Charter of Rights and Freedoms, and the Privacy Act (Canada). Mostly this legislation concerns privacy infringement by government organizations. Data privacy was first

[150] 428 U.S. 52(1976).
[151] 431 U.S. 678(1977).

addressed with the Personal Information Protection and Electronic DocumentsAct, and provincial-level legislation also exists to account for more specific cases personal privacy protection against commercial organizations. Classically understood as the 'right to be left alone,' privacy in today's high-tech world has taken on a multitudeof dimensions. In its broadest sense, privacy is equated with the right to enjoy private space, to conduct private."

"Communications, to be free from surveillance and to respect the sanctity of one's body. To most people, privacy is about control – what is known about them and by whom. Privacy protection in this country, however, is focused on the safeguarding of personal information or data protection. Drawing upon generally accepted fair information practices, federal laws seek to allow, to the greatest extent possible,individuals to decide for themselves with whom they will share their personal information, for what purposes and under what circumstances. Thus, what is an unacceptable privacy intrusion to one person may not be to another."

"Privacy is regulated at both the federal and provincial level. At the federal level,privacy is protected by two acts: the 1982 federal Privacy Act and the (PIPEDA)"[152]. "The federal Privacy Act of 1982 regulates the collection, use and disclosure of personal information held by federal public agencies and provides individuals a right of access to personal information held by those agencies, subject to some exceptions, including an exemption for court records. Individuals can appeal to a federal court. Individuals may request records directly from the institution which has the custody of the information. Accessible information includes written records, video and computer files. The Act establishes a code of fair information practices which apply to government handling of personal records. The Privacy Act and the Access to Information Act are overseen by independent commissioners with the power to investigate, mediate and make recommendations, but with no ability to issue binding orders. However, a commissioner can initiate a Federal court review if it believes an individual has been improperly denied access."[153]

"Other federal legislations also have provisions related to privacy. The Telecommunications Act 1993 has provisions to protect the privacy of individuals,

[152] Personal Information and Electronic Documents Act, 2000.
[153] Hunter v. Southam, 2 Supreme Court Reports.

including the regulation of unsolicited communications. Also the Bank Act, Insurance Companies Act and Trust and Loan Companies Act, permit regulations to be made governing the use of information provided by customers. There are Sectoral laws for pensions, video surveillance, immigration and social security. The young offenders Act regulates what information can be disclosed about offenders under the age of eighteen while the corrections and conditional release Act speaks to what information can be disclosed to victims and victims' families. In addition, most provinces have some form of legislation protecting consumer credit information. However, the vast majority of information collected by the private sector is on the provincial level and is not currently protected by any provincial Laws."[154]

"Currently, neither federal privacy law applies to Parliament. The Privacy Act applies only to 'government institutions,' which are defined (in section 3) as all of the government departments, bodies and offices listed in the Schedule to the Act. In 1997, the House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities recommended that federal data protection legislation should apply to Parliament. In 2000, following a comprehensive review of the Privacy Act, the Privacy Commissioner of Canada recommended that the House of Commons and the Senate be included among the list of institutions subject to the Act. There has, however,been no subsequent legislative action in this regard. As a result, parliamentary employees and the general public do not have rights under the Act to their personal information held by a parliamentary institution or parliamentarian."[155]

In January 2001, "the Data Protection Working Party of the European Commission issued a decision stating that PIPEDA (Personal Information and Electronic Documents Act) provided an adequate level of protection for certain personaldata transferred from the EU to Canada. This will allow certain personal data to flow freely from the EU to recipients in Canada subject to PIPEDA without additional safeguards being needed to meet the requirements of the EU Data Protection Directive.However, the Commission's decision of adequacy does not cover any personal data heldby the federal sector or provincial bodies or information held by personal organizations and used for non-commercial purposes, such as data handled by charities or collected inthe context of an

[154] Lavigne v. Canada (Office of the Commissioner of Official Languages), 214 D.L., R215(2000).

[155] Privacy Commissioner of Canada, Privacy Act Reform: Issue Identification and Review, 16 June 2000.

employment relationship. Operators in the EU will have to put in place additional safeguards, such as the standard contractual clauses adopted by the Commission in June 2001 before exporting the data to these organizations." [156]

In May 2002, "Canada became the first national government to make privacy assessments by federal departments and agencies mandatory. The Privacy Impact Assessment Policy means that all new and existing federal programs and services with potential privacy risks will undergo a Privacy Impact Assessment (PIA). The goal is a comprehensive report that ensures that privacy protection is a core consideration in the initial framing of program or service objectives and in all subsequent activities. According to the policy, the Office of the Privacy Commission will review all Privacy Impact Assessments and offer comments to departments at an early stage."[157]

"Privacy legislation on a provincial level is separated into three categories:

a. public sector (data protection) law,
b. private sector law and
c. sector-specific laws.

Public sector legislation covering government bodies exists in almost all provinces and territories. Nearly every province has some sort of oversight body, but they vary in their powers and scope of regulation. New Brunswick and Prince Edward Island were the last provincial governments to introduce provincial public sectorlegislation. With the passing of these two acts, every territory and province in Canada, except Newfoundland and Labrador, will have statutory protection for personal information held by government agencies. Most provinces address both accesses to information and privacy issues in the same legislation. With respect to provincial sectorspecific legislation, many provinces have specific laws to protect personal information,including health-specific privacy laws, consumer credit reporting laws, laws regulatinginformation from credit unions, and legislation imposing restrictions on the disclosure of personal information held by private investigators and other professionals. Alberta, Manitoba, and Saskatchewan have all passed health-specific privacy legislation, whichsets rules for

[156] European Union Data Protection Working Group - Article 29, Opinion 2/2001 on the Adequacy of the Canadian Personal Information and Electronic Documents Act.

[157] Treasury Board of Canada Secretariat, "Privacy Impact Assessment Report, available at http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paip-pefr_e.asp. Visited on 20th of December 2022, at 11.55pm.

the collection, use, and disclosure of personal health information. These laws apply to personal health information held by hospitals, government ministries, regulated health professionals, and other health care facilities. As of January 1, 2004, the federal PIPEDA applied to all commercial activity in provinces unless the provinceenacted 'substantially similar' laws."[158]

Arguably, "there is always the possibility of privacy infringement claims in relation to Parliament pursuant to sections 7 and 8 of the Canadian Charter of Rights and Freedoms. While Canadians have no express constitutional right to privacy, the courts have interpreted sections 7 and 8 of the Charter as guarding against unreasonable invasions of privacy. Section 7 provides for the right to life, liberty and security of the person and the right not to be deprived of these rights except through some form of due process. Section 8 protects against unreasonable search and seizure. The privacy value in these rights, however, has largely been recognized in the criminal law context. It is for this reason, among others, that calls continue to be made for the entrenchment of an explicit and broad right to privacy in the Canadian Constitution."

All that being said, "it has generally been the practice of parliamentary institutions and parliamentarians to respect the principles of federal human rights legislation, particularly when the courts have recognized such legislation as quasi constitutional. As the Supreme Court of Canada pointed out in *Canada (House of Commons)* v. *Vaid*[159], legislative bodies created under the Constitution 'do not constitute enclaves shielded from the ordinary law of the land,' and parliamentary privilege only functions to provide 'necessary immunity' for legislators to do their work. Thus, although Parliament in its wisdom has chosen not to include itself within the ambitof the federal Privacy Act, best policies and practices would certainly dictate that as a public institution accountable to the public, Parliament should strive to conduct itself ina manner consistent with that required of others in terms of protecting the privacy of personal information."

"Guidance in the application of fair information practices to the parliamentary context might therefore be drawn from the privacy principles set out in the federal Privacy Act.

[158] A list of provincial and territory privacy laws and commissions, available at this site - http://canada.justice.gc.ca/en/ps/atip/provte.html. Visited on 25th of December 2022 at 10.15pm.
[159] 1 S.C. 667(2005).

The Act incorporates the basic tenet underlying most data protection laws,which is that an individual's personal information is his or hers to control. The law stipulates that only personal information related directly to an operating program or activity of government may be collected. It also requires that, wherever possible, the information be collected directly from the individual concerned, that the individual be informed of the purpose of the collection, and that the information be used or disclosedonly for the purpose for which it was collected unless the individual consents or the legislation provides otherwise".

Right to Privacy with Judicial Law

In Canada, "experimentation with privacy remedies at the provincial level has led to growing acceptance of a right to privacy nationwide. Quebec[160] has extended its version of the civil law actio injuriarum to invasions of privacy and 0ntario and Albertahave allowed damage actions and injunctive relief based on a right to privacy. Three provinces, British Columbia, Manitoba and Saskatchewan have enacted statutes making willful violation of privacy a tort. Under these statutes, the Canadian courts have begun to work out the scope of the new statutory right.[161] The federal legislature has made wire-tapping and electronic eavesdropping criminal offences under a 1973 Protection of Privacy. The federal statute applies to official interceptions, rendering them unlawful and inadmissible in evidence unless specifically authorized by a judge applying very narrow criteria of overriding public interest. The Act further provides that punitive damages may be awarded to the victim of an unlawful interception."[162] Although many provinces lack general privacy legislation, the combined effect of the extant common law, and provincial and federal legislation, grants Canadians a fair measure of privacy protection, 'perhaps as great as the United States' where the common law right to privacy originated.

In 1998 the Supreme Court of Canada found that a young woman's privacy hadbeen invaded through the publication of her photo without her consent, despite the factthat the photo was taken of her sitting on the steps of a public building in a public place.[163] "The puzzle of this case is to understand how the fact of taking a photo and publishing

[160] Robbins v. CBC 12 DLR 32(1957).
[161] Davis v. McArthur 17 DLR 760(1971).
[162] Section 178, Protection of Privacy Act 1973.
[163] United States Dept. of Justice v. Reporter Commission for Freedom of the Press. 489 U.S. 749(1989).

it transforms an ostensibly public act – sitting in a public place -into one thatattracts a privacy interest. Nine years earlier, the United States Supreme Court held that the compilation of matters of public record attracted a privacy interest, given the ease of access facilitated by the aggregation of data through computer technology." In the Reporters case, computer technology allows information to be aggregated and it is this aggregation that accounts for the court's willingness to protect it. The ability of technology to move information from one context to another as well as to aggregate date therefore go to the heart of what concerns us about the uses of information in the contemporary context.

"There is no explicit right to privacy in Canada's Constitution and Charter of Rights and Freedoms. However, in interpreting Section 8 of the Charter, which grants the right to be secure against unreasonable search or seizure, Canada's courts have recognized an individual's right to a reasonable expectation of privacy. Section 8 of the Canadian Charter of Rights and Freedoms guarantees the right to be secure against unreasonable search or seizure"[164]. Ever since *Hunter* v. *Southam*[165], this provision has been interpreted to protect a "reasonable expectation of privacy". "In principle, such a test is compatible with a sensitivity to context and so holds out the promise of coming to terms with the salient features of information technology."

"It is not yet clear to what extent the Canadian common law courts will recognizea right to privacy in public places. Certainly the American approach has been influentialin some Canadian cases. In *Davis* v. *McArthur*[166], the British Columbia Court of Appealappears to have accepted that surveillance in public places could potentially breach the Privacy Act even where there is a legitimate interest in the plaintiffs conduct, although it concluded that the shadowing and observation in the instant case were 'not so close and continuous as to go beyond reasonable bounds."

In *Ontario (A.G.)* v. *Dieleman*,[167] "the Ontario Court considered an argument that picketers who drew attention to women entering abortion clinics were invading their privacy. Adams J. looked to the American cases and to Professor Prosser's observations about the lack of privacy protection in public places and noted that, factually, the

[164] Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, 1982.
[165] 2 S.C., R 145(1984).
[166] 17 D.L., R 760(1970).
[167] 117 D.L., R 680(1994).

picketing was on public sidewalks, so the defendants were able to assert that there was nothing 'private' about these locations. However, the Court did not reach a conclusion on the privacy issues, instead granting an interlocutory injunction based on public and private nuisance."

In *Aubry* v. *Editions Inc*.[168] "the Supreme Court of Canada upheld adecision of the Quebec courts awarding $2 000 damages to a young woman whose photograph was published in an artistic magazine. The photograph was taken without her consent as she sat on a step outside a building on a Montreal street. The Court heldthat the publication constituted a fault under Quebec law, as a fault is committed as soonas an identifiable image of a person is published without consent, unless justified by thepublic interest. The majority also believed there was sufficient proof of damage. The majority judgment discussed situations in which the right to privacy in a public place would be outweighed by the public interest, such as where the person appears in only an incidental manner and is not the principal subject of the photograph."

"However, such situations were seen as the exception rather than the rule, and the view that there was an unlimited right to publish photographs taken in a public placewas expressly rejected. It remains to be seen how much impact the Aubry decision willhave in the common law jurisdictions.

There are other indications that Canadian law may be more receptive than American law to the notion of public privacy. In *Dagg* v. *Canada (Minister of Finance),*[169] the Supreme Court of Canada held that time entries in sign-in logs, recording when employees entered and left the workplace on weekends, constituted 'personal information' for the purposes of Sec 3 of the federal Privacy Act. La Forest J.stated, 'In my view, a reasonable person would not expect strangers to have access to detailed, systematic knowledge of an individual's location during non-working hours, even if that location is his or her workplace. He noted that even in the search and seizurecontext, in which 'the countervailing state interest in surveillance may be very strong,' there has been some recognition of a privacy interest in a person's physical movements.Dagg is especially significant because a person's movements are perhaps the most basic information revealed when appearing in a public place."

[168] 1 D.L., R 577(1998).
[169] 2 D.L., R 148(1997).

The British Columbia Information and Privacy Commissioner has recognized the vulnerability to privacy invasion of people filmed in interactions with the police in public places. “KF Media Inc. v. Vancouver (police department),[170] Commissioner investigated a complaint from the producers of ‘To Serve and Protect’, a 'reality television' show about day-to- day police work. The complaint concerned a decision of the Vancouver Police Department that the show could no longer reveal the identities of persons videotaped in public during 'ride a longs.' The Commissioner affirmed the Department's policy and recommended that any police department that allows a film crew to accompany its officers on duty should require the production company to obscure the identities of members of the public before broadcast. He also commented that persons in contact with the police cannot give voluntary and informed consent to the disclosure of their identities when they are under great stress and may be incapacitated or intoxicated. stress and may be incapacitated or intoxicated.”

In summary, “the reaction of Canadian decision makers faced with claims to privacy in public places has varied widely. Although American privacy cases have beeninfluential, and a distinctly paranoid view has been adopted in at least one Canadian decision, nevertheless there are signs that Canadian courts may be more open to the notion of public privacy. Parliament, its institutions, members and staff will most certainly encounter situations where choices have to be made about the handling of personal information. In making these choices, reference to the fair informationprinciples set out in Canada’s privacy statutes may prove helpful. Consideration mightalso be given to the possible benefits of privacy promotion and protection in terms of fostering public support and confidence. Indeed, at a time when government accountability and transparency is a public priority, assuring Canadians that their informational privacy rights are respected might not only be good for parliamentary records management and employee/public relations, but it could also contribute to a healthy and meaningful democracy.”

Japan

Statute Protection of Right to Privacy

Article 21 of the 1946 Constitution states: -

[170] 2 N.Z.L., R 728(1995).

1. Freedom of assembly and association as well as speech, press and all other formsof expression are guaranteed.

2. No censorship shall be maintained, nor shall the secrecy of any means of communications, be violated. Article 35 states

3. The right of all persons to be secure in their homes, papers and effects againstentries, searches and seizures shall not be impaired except upon warrant issued for adequate cause and particularly describing the place to be searched and thingsto be seized.
4. Each search or seizure shall be made upon separate warrant issued by a competent judicial officer.[171]

Westin and Horibe[172] "both pinpoint the elevation of privacy protection to the national political agenda to a research initiative in the Administrative Management Agency in 1981.This agenda led to the passage of Japan's original sectoral legislation, the 1988 Act for the Protection of Computer-Processed Personal Data held by Administrative Organs (Act No. 95 of 1988). The 1988 Act for the Protection of Computer Processed Personal Data Held by Administrative Organs (the 1988 Act) governs the use of personal information in computerized files held by government agencies."[173]

"The Act is based on the OECD Privacy Guidelines and imposes duties of security, access, and correction. Agencies must limit their collection to relevant information and publish a public notice listing their file systems. Information collectedfor one purpose cannot be used for a purpose 'other than the file holding purpose.' The1988 Act is overseen by the Government Information Systems Planning Division of the Management and Coordination Agency. The agency does not have any powers to investigate complaints. The 1988 Act was totally amended and enacted as the Act for Protection of Personal Data Held by Administrative Organs."

[171] Constitution of Japan, Nov. 3, 1946 available at http://www.ntt.co.jp/japan/constitution/englishconstitution.html. Visited on 25th of December 2022 at 04.30am.

[172] Westin and Masao Horibe, 'Privacy and Personal Information Protection in Japan: Past, Present and Future'.

[173] The Act for the Protection of Computer Processed Personal Data Held by Administrative Organs,Act No. 95, 16 December 1988 (Kampoo, 16 December 1988) available at - http://www.ntt.co.jp/japan/constitution/englishconstitution.html. Visied on 26th of December 2022 at 02.30pm.

"The new act governs paper-based data as well as computerized data, and sets new criminal provisions for government officials who leak personal information without proper justification. Japan is a member of the Organization for Economic Cooperation and Development and a signatory to the OECD Guidelines on Privacy and Transborder Data Flows. Japan participated as a nonmember observer country in the negotiations on the Council of Europe Convention on Cybercrime and signed the Convention in November 2001."[174]

"Other sectoral laws were enacted from the late 1980s to provide standards for the handling of financial, credit and employee information by the private sector, but the largely self-regulatory agenda prevailed until the late 1990s. Businesses operated in the shadow of influential ministerial guidelines issued by the Ministry of International Trade and Industry, the Ministry of Foreign Affairs and the Ministry of Posts and Telecommunications.

The government also actively fostered privacy mark systems and encouraged peak industry bodies to issue further private guidelines. The Electronic Commerce Promotion Council ('ECOM'), a body established in 1996 with connections to the Ministry of Economy, Trade and Industry ('METI'), first issued its own guidelines in 1998. A 2000 ECOM charter communicated a deep sense of foreboding and urgency that Japan may be left out of global prosperity without rapid regulatory change to facilitate e-commerce."[175]

Right to Privacy with Judicial Law

"Privacy protection is now firmly part of the mainstream political agenda in Japan and predicts that it is likely to succeed in much the same manner as environmentalprotection has, utilizing informal regulatory mechanisms.

In addition to 'soft' moral merits, both have 'hard' connections to Japan's future prosperity. This makes privacy a new, but integral, Japanese societal value, irrespective of the vague or hortatory aspects of the regime.

The formidable Japanese bureaucracy has been appointed as a Cerberean privacy watchdog and will act effectively or face the wrath of the nation. This forceful political

[174] The Act for Protection of Personal Data Held by Administrative Organs of 2003, Art. 53-55.

[175] Electronic Commerce Promotion Council of Japan, Outline of A Survey of the Market Scale for Electronic Commerce (1999) available at http://www.ecom.jp/qecom/ecom_e/index.html. Visited on 27th of December 2022 at 07.20pm.

agenda, responsive to popular demand, speaks of an increasingly empowered Japanese citizen, even if for economic reasons rather than lofty ideals concerning human rights and civil liberties. Increasingly empowered citizens mean the developmental state model of the Japanese polity is an increasingly uneasy fit and the pluralist and participatory democracy model is gradually becoming more alter."

Germany

Statute Protection of right to PrivacyArticle 1 (Protection of human dignity)

1) Human dignity shall be inviolable. To respect and protect it shall be the duty ofall state authority.

2) The German people therefore acknowledge inviolable and inalienable humanrights as the basis of every community, of peace and of justice in the world.

3) The following basic rights shall bind the legislature, the executive, and thejudiciary as directly applicable law.

Article 2 (Rights of liberty - personal freedoms)

1) Every person shall have the right to free development of his personality insofaras he does not violate the rights of others or offend against the constitutional order or the moral law.
2) Every person shall have the right to life and physical integrity. Freedom of the person shall be inviolable. These rights may be interfered with only pursuant toa law.

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 bya review of the case by agencies and auxiliary agencies appointed by the legislature.

Article 13 (Inviolability of the home)

1) The home is inviolable.
2) Searches may be authorized only by a judge or, when time is of the essence, byother authorities designated by the laws, and may be carried out only in the manner therein

prescribed.

3) If particular facts justify the suspicion that any person has committed an especially serious crime specifically defined by a law, technical means of acoustical surveillance of any home in which the suspect is supposedly staying may be employed pursuant to judicial order for the purpose of prosecuting the offence, provided that alternative methods of investigating the matter would be disproportionately difficult or unproductive. The authorization shall be for a limited time. The order shall be issued by a panel composed of three judges.

   When time is of the essence, it may also be issuedby a single judge.

4) To avert acute dangers to public safety, especially dangers to life or to the public, technical means of surveillance of the home may be employed only pursuant tojudicial order. When time is of the essence, such measures may also be ordered by other authorities designated by a law; a judicial decision shall subsequently be obtained without delay.

5) If technical means are contemplated solely for the protection of persons officially deployed in a home, the measure may be ordered by an authority designated by a law. The information thereby obtained may be otherwise used only for purposes of criminal prosecution or to avert danger and only if the legality of the measure has been previously determined by a judge; when time isof the essence, a judicial decision shall subsequently be obtained without delay.

6) The Federal Government shall report to the Bundestag annually as to theemployment of technical means pursuant to paragraph (3) and, within the jurisdiction of the Federation, pursuant to paragraph (4) and, insofar as judicial approval is required, pursuant to paragraph (5) of this Article. A panel elected by the Bundestag shall exercise parliamentary control on the basis of this report.

7) Interferences and restrictions shall otherwise only be permissible to avert a danger to the public or to the life of an individual, or, pursuant to a law, to confront an acute danger to public safety and order, in particular to relieve a housing shortage, to combat the danger of an epidemic, or to protect young persons at risk.

Article 18 (Forfeiture of basic rights)

Whoever abuses the freedom of expression, in particular the freedom of the press (paragraph (1) of Article 5), the freedom of teaching (paragraph (3) of Article 5), the freedom of assembly (Article 8), the freedom of association (Article 9), the

privacy of correspondence, posts and telecommunications (Article 10), the rights of property (Article 14), or the right of asylum (Article 16a) in order to combat the free democraticbasic order shall forfeit these basic rights. This forfeiture and its extent shall be declaredby the Federal Constitutional Court.

Article 19 (Restriction of basic rights)

1) Insofar as, under this Basic Law, a basic right may be restricted by or pursuant to a law, such law must apply generally and not merely to a single case. In addition, the law must specify the basic right affected and the Article in which itappears.
2) In no case may the essence of a basic right be affected.
3) The basic rights shall also apply to domestic artificial persons to the extent thatthe nature of such rights permits.
4) Should any person's rights be violated by public authority, he may have recourseto the courts. If no other jurisdiction has been established, recourse shall be to the ordinary courts. The second sentence of paragraph (2) of Article 10 shall notbe affected by this paragraph.

On 3 October 1990 Germany achieved national unity. By virtue of a sovereign, conscious decision of the people, the Basic Law became the constitution for the whole nation. The successful democratic revolution in the former German Democratic Republic had achieved its goals: human dignity, civil rights, fundamental freedoms and democracy for the entire German people in a society based on the rule of law tempered by social justice."[176]

"Germany has one of the strictest data protection laws in the European Union. The world's first data protection law was passed in the German Land of Hessen in 1970.In 1977, a Federal Data Protection Law followed, which was reviewed in 1990, amendedin 1994 and 1997. The final revision took place in 2002 to be in line with the EU Data Protection Directive. The general purpose of this law is 'to protect the individual against violations of his personal rights by handling person-related data.' The law covers collection, processing and use of personal data collected by public federal and state authorities (as long as there is no state regulation), and by non-public offices, if they process and use data for commercial or professional aims. The Federal Data Protection

[176] Available at www.gilc.nl/privacy/survey/surveyak.html. Visited on 19th of December 2022 at 11.00pm.

Commission is an independent federal agency that supervises the Federal Data Protection Act. Its chief duties include receiving and investigating complaints, as well as submitting recommendations to parliament and other governmental bodies. The Federal Data Protection Commission publishes an annual activity report." [177]

"Another important federal law in Germany is the G-10 law, which imposes limitations on the secrecy of certain communications. The G-10 law was amended in 2001 to require that service providers give law enforcement the means to monitor data as well as voice lines. Wiretapping is also regulated by the G-10 law and requires a courtorder for criminal cases.

Germany is a member of the Council of Europe and has signed and ratified the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108) and later signed an Additional Protocol to this convention. It has also signed and ratified the European Convention for the Protection of Human Rights and Fundamental Freedoms. In November 2002 Germany signed the Convention on Cybercrime. It is a member of the Organization for Economic Cooperation and Development and has adopted the OECD Guidelines on the Protection of Privacy and Trans border Flows of Personal Data."[178]

Right to Privacy with Judicial Law

"Germany has extremely strict privacy laws. The supreme court hasacknowledged a right to 'informational self-determination' and everyone storing personal data about others has to obtain consent from these persons, has to allow them access to their records, and can use the data only for the purpose they were originally collected for. The federal government and all states have privacy ombudsmen who takecitizen's complaints and make sure that the privacy laws are enforced and extended where appropriate. Germans value their privacy highly and essentially everybody agreeswith these laws. A controversial state law allowing the government to spy on a citizen'shard drive using virus-like software has been struck down by Germany's highest court. The German Constitutional Court, in the southwestern city of Karlsruhe, said on Wednesday that a surveillance law passed in 2007 in the state of North Rhine- Westphalia was too

[177] Federal Act on Data Protection ("BDSG").

[178] Christopher Millard & Mark Ford: Data Protection Laws of the World, Sweet and Maxwell,Vol.1,2000.

broad. The law gave security officials the authority to spy remotely on suspected criminals by sending a computer virus that would read data from a suspect's hard drive. The law permitted not just access to the hard disk but also ongoingsurveillance of data, such as e-mail, as well as remote tracking of keyboard entries or online phone calls. This activity, the court said, violated a person's right to privacy. Butthe decision allowed for exceptions: in cases of 'paramount importance' - that is, in cases of life or death, or a threat to the state -- authorities would be permitted to use suchsoftware, with a court's permission."[179]

Privacy is one of the truly profound values for a civilized society. "In free societies, the community ostensibly Speaks through a popularly constituted government. Thus, government protection of privacy rights is a measure of a society's commitment to liberty and, in a broader sense, autonomy. Privacy law reflects the tolerance of a nation. Although privacy is only one example of autonomy, privacy rights are a substantial subset of personal autonomy. Thus, examining privacy rights is one way to evaluate the general measure of liberty a society confers on its members. But, even if one recognizes the need for privacy, the right of privacy cannot be absolute. The existence of political community requires the relinquishment of certain rights, prerogatives, and freedoms." As John Locke described, individuals must cede some rights and prerogatives that they otherwise could claim in a lawless state of nature: "Whosoever therefore out of a state of Nature unite into a Community, must beunderstood to give up all the power, necessary to the ends for which they unite into Society, to the majority of the Community Nevertheless, Democratic societies strive to maximize freedom while simultaneously ensuring the survival of the institutions thatsecure the liberties of the people. Thus, individuals in democratic states expect community deference to some choices. The right of privacy is one way to articulate thisexpectation of autonomy. There is a growing trend towards the enactment of comprehensive privacy and data protection legislations around the world." Currently over forty countries have or are in process of enacting laws on the right to privacy.

[179] Niemietz v. Germany, ECHR,16june 1992.

Chapter - 4

Constitutional Right to Privacy in Cyber Age

Advances in Information and communication technology substantially improve communication and information exchange in real time. It promotes democratic involvement by enhancing access to information and encouraging global discourse. These strong technologies provide promises to promote the enjoyment of human rights by amplifying and revealing the voices of human rights defender.

However, it is also evident that these new technologies are vulnerable to electronic monitoring and interception. Recent findings have shown how new technology are created hidden, frequently with a chiller effect, to assist these actions.[180]

In this backdrop it is essential to analyze the human rights issues in digital environment, especially the online personal data privacy. It is necessary to verify that whether digital world respect the human rights while dealing with data of private nature. The researcher has aimed to explore his fourth objective of studying to study human rights violations due to cybercrimes and inadequate cyber laws guarding personal data and online privacy further their data. The necessity of harmonization or even standardization, in data protection standards is also ratcheted by big data. Because personal information is gathered and exchanged widely across sectors oral and national boundaries, uneven privacy rules are placing more and more individuals, organizations and society at risk. The greatest consequence of big data may be the pressure it exerts on fresh, deliberate, informed worldwide debates on the core concepts underlying data protection.

As for the Indian law, not only before big data, but also before, mobile computers, GPS, smart phones, tablets or many other developments made it possible for big data and the legislation of India to be redundant.[181]

---

[180] See for details, http://www.ohchr.org/EN/lssues/DigitalAge/Pages/DigitalAgel n dex.aspx, Visited on 19th of December 2022.

[181] Christopher Kuner, Fred H. Cate, Christopher Millard and Dan Jerker B. Svantesson "The challenge of 'big data' for data protection" Oxford Journals, International Data Privacy Law,

Thus such issues give much scope of discussion on human rights issues regarding privacy in present environment. Because it has been contended that most of the privacy laws and growth of the concept has been taken place in the paper based environment, but as the digital environment play much role in the life of an individual, the discussion on privacy and rights related thereto provide much scope for its exploration.

Online Data privacy - Whether a fundamental human right?

Human rights are the fundamental rights that are inalienable and necessary to human life. Human rights are human rights, regardless of nationality, race, creed, sex etc. just because he or she is a human being.[182] In accordance with natural law, people do not obtain human rights from social order or from societies. They are naturally independent of people and even before their involvement in civilization. Now the questions arises which rights can be termed as human rights? The answer to this question is difficult as there is no set of entire human rights listed anywhere. Different schools of law have defined human rights in their own fashion and have recognized different rights as human rights. At international level till date numerous efforts have been made to set out the list of human rights. For example English Bill of Rights, 1689 French Declaration, 1789 Universal Declaration of Human Rights, 1948 Covenants on Civil, Political rights, 1966 Economic, Social and Cultural rights 1966 and many more. At national level most of these human rights have found place in the Constitution, statutory legislations or by judicial expansion of fundamental rights and directive principles enshrined in the Constitution. No matter which forum is discussed national or international or be it in the writings of jurists or philosophers one right has always found a prominence.

Seat inside, i.e. private right. It is incorporated, at international level, in Article 8 of the European Convention on Human Rights, Article 17 of the International Pact on Civil and Political Rights, etc. There is no particular right to privacy as such under the Constitution. However, Article 21 of this right was abrogated by the Supreme Court

http://idpl.oxfordjournals.org/content/2/2/47.fullol 2 Issue 2 http://idpl.oxfordjournals.org, 25th of December 2022.

[182] What are human Rights, Available at: http://www.ohchr.org/en/ issues/pages/whatarehu man rights.Aspx (Visited on August 12, 2022).

and numerous other Constitutional Articles read with the State Policy Directive Principles.[183] Right to life does not mean life barely of animal existence, it means much more. It denotes those conditions of life which develops an individual, so that he can live his life to the fullest extent. Development should not only be in terms of material or fiscal but also intellectual, moral, ethical, spiritual, social and more. Such development is not possible without guaranteeing right to privacy.

The nature of Right to Privacy like any other right is not static but a dynamic one. It changes it color as per the context in which it is taken. We may say that it changes from time to time and place to place and person to person. In earlier days scope of privacy was very limited. The law regulating it was also scattered everywhere and it was not recognized as an independent right in itself. Common law protected right to privacy in terms of law prohibiting trespass and defamation etc. Artistic work of an artist was not only subject to copyright law but was also regarded as his private work and hence his right to privacy over his creations. Photographs of people clicked in their private moments if published in public was regarded as serious violation of privacy and so was tapping of telephone calls between two persons having a personal conversation. As time progressed angle of privacy protection became wider. Test of virginity,[184] publication of medical records, [185] domiciliary visits in night at residence[156] all were considered as violation of fundamental right to privacy. It is clear that privacy protection includes in itself protection of personal data also. Personal data and privacy are whole and part of each other i.e. It cannot be separated since personal data is simply information on the person identified or identified (Data Subject) identified, directly or indirectly, by references in particular to the person's identification number, or to a physical, physiological, mental, economic, cultural or social factors specific to him/her.[186] The security to be extended to right of privacy similarly has to be extended to protection of personal data also. As personal data is part and parcel of human personality and a key ingredient in his development personal data privacy becomes another facet of right to life and liberty and hence a fundamental human right. Having said all this development of science and technology especially information communication technology has posed

[183] M.P Jain, Indian Constitutional Law 1133 (Wadhwa and Company, Nagpur, 5th Edn.,2008).
[184] Surjit Singh. v. Kawaljit Kaur AIR 2003 PH 353.
[185] Mr X v. Hospital Z Appeal (civil) 4641. of 1998.
[186] Gobind v. State of M.P AIR 1975 SC 1378.

some new challenges. Advent of internet has connected computer to every other computer in the world through cyberspace. Computer which contains personal data, when connected to internet becomes accessible to whole world.

Information communication technology has made people too dependent upon the computers and internet and despite the danger of being exposed to world and losing privacy (by losing personal data) in public domain people have no option at hand. Her Jaw should strike a balance and should stop information technology from being misused.

If the predominant theoretical viewpoint of privacy is taken from the human rights history, one will not submit to too widespread generalisation. Although this strategy is unlikely to be replaced, there are also different viewpoints. It is impressive to recognise privacy as a moral and social value.[187] As stated by the "Standing Committee on Human Rights and the Status of Persons with Disabilities": "Privacy is a core human value that goes to the very heart of preserving human dignity and autonomy."[188] It also helps to achieve broader societal goals that improve social welfare in general. In practical terms, in countless encounters and transactions, privacy must be respected and taken into account in the public sphere. This can be done by adopting or observing a set of rules governing the handling of personal information, and there should be consensus that this set of rules should consist of what is sometimes called fair information practices. [189] . These principles implicitly apply if personal information is gathered, utilized or released in all settings by the prescription. In essence, such fair information practices lay forth information privacy rights, giving a foundation for interaction connections, between the person and the company who gathers uses or communicates personal information.

---

[187] Ann Cavokian, "Privacy as a Fundamental right v. Economic right : An attempt at conciliation," Available at: http://www.ipc.on.ca/images/Resources/up-lpr _right.pdf last (Visited on May 11, 2022).

[188] Canada, Standing Committee on Human Rights and the Status of Persons with Disabilities, Third Report, Available at: http://ww w .parl.gc.ca? committ e es3 52/ husoreports/ 03_1997-04/a pp le. html (Visited on June 14, 2022).

[189] "Fair information practices" were articulated internationally in 1980 when the Organization for Economic Cooperation and Development issued its document, Guidelines on the Protection of Privacy and Tran-border Flows of Personal Data, 1960 and consist of a number of privacy or data protection principles.

Privacy has always been a matter of concern at International level. Current international human rights jurisprudence is a outcome of efforts taken for centuries altogether. They are outcome of some famous revolutions and efforts taken by world community after witnessing two devastating world wars. During these phases right to privacy has always found its place in one form or the other. For example in land mark cases like Griswold v. Connecticut, which struck down a law banning contraceptives and Roe v. Wade, which established a woman's right to an abortion Right to Privacy was recognized and valued. In Planned Parenthood v. Casey the Court strike down abortion law and upheld limited right to abortion as abortion was a personal affair and state had no role to play.

Similarly after creation of United Nations there have been number of International covenants and conventions which strived to protect all forms of privacy.

There was a danger that the free flow of personal data across borders could be impeded by differences in national legislation; in recent years this has increased considerably and will continue to increase with the widely used introduction of new computers and communication systems. Limiting flows might lead in critical economic areas such as banking and insurance to major disruption that is why the OECD Member States have found it important to adopt guidelines to help harmonies national data protection laws and minimize disruptions of international data flows This constitutes an agreement on fundamental concepts that may be included into or used as a foundation for law in those nations that do not yet have national laws.[190] Regional co-operation like South Asian Association for region Co-operation misses out on forming a common opinion for protection of data during trans-border flow. Council of Europe: Recommendation No R(99) S from a Committee of Ministers on Internet Guidelines to Protect Persons With Concerning Collecting and Processing Personal Data on Right to Information Highways to Member States to protect privacy. The focus is on examining the evolution of technology to help towards protecting basic rights and freedoms and, in particular, privacy while processing personal information involving natural beings. The aim is to

[190] OECD Guidelines on Privacy ieconomy/oedgudelinesonth eprotectio nofprivacyandtrn nsborderfl owsofpersonaldata.htm(Visited on March 15, 2021).

highlight the need for the development of techniques which will allow anonymity of data subjects and for information exchanged on information routes to be treated confidentially while respecting other people's rights and freedoms and the ideals of a democratic society and acknowledging that communication utilising the new technologies of information must also be respectful of people. It stresses on recognizing that the collection, processing and especially communication of personal data by means of new information technologies, particularly the information highways, are governed by the provisions of the Convention for the Protection of Individual with regard to Automatic Processing of Personal Data (Strasbourg 1981, European Treaty Series No. 108) and by sect oral recommendations on data protection and notably Recommends No R (90)19 on the protection of personal data used for payment and other related activities, No R (91) 10 on communications by public bodies to third parties of personal data and No R(95) 4 on personal data protection in the areas of telecommunications with a particular reference to telephone services. Tele Communications Services. Council report on cross-border cooperation in the field of law enforcement protecting privacy OECD Recommendation.

The aim of this recommendation was to create international cooperation between the privacy authorities to solve the issues of safeguarding persons' personal information, wherever the data or persons are situated. This recommendation it showed the Member States' resolve to upgrade their enforcement systems and legislation where necessary in order to enhance their data protection efficiency.

Another Protocol to the Convention for the Protection of Persons on the Automatic Processing of Personal Data on supervisory authorities and trans-border flows of data is structured taking account of the need to [191] ensure effective protection of human rights and fundamental freedoms by increasing exchange of personal data across borders.

"Declaration of Principles on Freedom of Expression in Africa, African Commission

[191] Council of Europe, available at: http://conventions.coe.int/ Treaty/Common/QueVoulezVous.as

on Human and Peoples' Rights," [192]32nd Session, 17 - 23 October, 2002: Banjul, The Gambia. Part IV (3) states that "Everyone has the right to access and update or otherwise correct their personal information, whether it is held by public or by private bodies and thus protects personal data privacy." Guidelines for the regulation of computerized personal data files passed by Resolution of General Assembly, 19[193] in addition to personal data protection principles.

These standards should be avoided and, if required, expressly provided for when the file is intended to safeguard personal or humanitarian aid's fundamental human rights and freedoms. The Convention on the Protection of Individuals in Automated Personal Data Processing aims at guaranteeing each individual, no matter what his/her nationality or residence or his/her rights to privacy and in particular to the automatic handling of personal data relating to his/her rights, in the territory of every Party ("data protection").[194]

Objective of Article 21

"In each case where a person complains of the deprivation of his life or personalliberty the court, in the exercise of its constitutional power of judicial review, has to decide whether there is a law authorizing such deprivation and whether in the given case, the procedure prescribed by such law is reasonable, fair and just, and not arbitrary,whimsical and fanciful".[195]

"The words except according to procedure established by law suggest that Article 21 doesn't apply where a person is detained by a private individual and not by or authority of the state, no fundamental right is infringement when the detention complained of is by a private individual. Article 32 also cannot be involved in such a case".[196]

[192] African Commission on Human and People's Right available at: http://www.achpr .org/sessions /32nd/resolutions/62/(Visited on May 5, 2021).

[193] Legislationline.org website, "A/RES/45/95", available at: http://www.legislationline .org /documents/ action/popup /id/6723 (Visited on May 11, 2021).

[194] Conventions.coe.int website, available at: http:/ /con vent ions.coe.int/TreatY /EN/Treaties/Html (Visited on February 11, 2021).

[195] Santosh Singh v. Delhi Administration, AIR 1973 Supreme Court 1091.

[196] Vidya Verma v. Shivnarayan Verma, 1955(2) SCR 983.

"Enjoyment of a quality life by the people is the essence if the guaranteed rightunder Article 21 of the Constitution.[197] But the protection of the Article external to all person not merely citizens[198] including even person under imprisonment".[199] "It also applies to preventive detention under Article 22. Article 21 doesn't refer only to the necessity to comply with the procedural requirements, put also to substantive right of acitizen. It aims as preventive measures as used us payment of compensation in case human rights of a citizen are cribbed.[200] Article 21 of the constitution provides for a safeguard in such a manner directing that FIR should be sent to the conversed courtwithin a period of 24 hours".[201]

Right to Life and Personal Liberty

"Article lays down that no person shall be deprived of life and personal liberty except according to 'procedure established by law' arose in famous *A.K Gopalan* v. *State of Madras*[202] where the validity of the Preventive Detention Act, 1950 was challenged. The question was whether Article 21 envisaged any procedure laid down bya law enacted by a legislature or whether the procedure should be fair and reasonable. On the behalf of Gopalan an attempt was made to persuade the Supreme Court to hold that the court could adjudicate upon the reasonableness of the Preventive Detention Actor for that matter, any law depriving a person of his personal liberty". Three pronged arguments were developed for this purpose: -

"The world 'law' incorporates principles of natural justice so that law deprivingthe life and personal liberty must incorporate the principles of natural justice. The reasonableness of the preventive law ought to be judged under Article 19, and The 'procedural due process.' However, the Supreme Court rejected all these arguments".

New Dimension of Right to Life

Supreme Court gave a new dynamic dimension to Article 21 and it was with thisdecision

[197] Hinch Lal Tiwari v. Kamla Devi, (2001) Supreme Court Case 496.
[198] Chairmam, Railway Board v. Chandrima Das, (2000) 2 Supreme Court Case 465.
[199] Sunil Batra v. Delhi Administrative, AIR 1978, Supreme Court 75.
[200] Bombay Dyeing and Wfs. Co.Ltd (3) v. Bombay Emital Action Group, (2006) 3 Supreme Court Case 434.
[201] Budh Singh v. State of U.P., (2006) 9 Supreme Court Case, 731.
[202] AIR 1950 Supreme Court 27: 1950 SCR 88.

the court started laying down a new constitutional jurisprudence. "Article 21 has characterized as the procedural magnacarta protective of life and liberty. For long, life and personal liberty occupied a back seat in India as accent was placed on propertyright. However, this situation has changed now. *Maneka Gandhi* v. *Union of India*[203] has brought the Fundamental right of life and personal liberty into prominence it is now regarded as the heart of Fundamental rights".

The expression life in Article 21 has been interpreted by Supreme Court rather liberally and broadly. "Over time, court has been given an expansive interpretation to life, the court has often quoted the following observation of Field, J., in *Munn* v. *Illinois*" an American Case: "By the term 'life' as here used something more is meantthan mere animal existence. Inhibition against its deprivation extends to all those limbsfaculties by which life is enjoyed."

Justice K.S. Puttaswamy v. *Union of India*,[204] "this is a recent case of Right to Privacy which was brought by 91-year old retired Karnataka High Court Judge Puttaswamy against the Union of India before a nine-judge bench of the Supreme to determine whether the Right to Privacy was guaranteed as a fundamental right under theIndian Constitution. This case was actually concerned with an issue to a challenge to the government Aadhaar scheme (a form of uniform biometrics-based identity card) in which the government made mandatory for availing the government services and benefits. The issue was made before a three-judge bench of the Supreme Court on the basis that this scheme violated the right to privacy. Accordingly, a Constitution Bench was set up and concluded that there was a need for a nine-judge bench to determine whether there is a fundamental Right to Privacy within the provision of Article 21 of Constitution of India".

"It was argued by the petitioner before the bench that Right to Privacy is a Fundamental right and should be guaranteed as right to life with dignity under Article 21 of the Constitution. Submissions made by the respondent were that the Constitution only recognized personal liberty which may include Right to Privacy to a limited extent".[205]

[203] AIR 1978 Supreme Court 597: 1 Supreme Court Cases 248.

[204] (2017) 10 SCC 1.

[205] http://www.legalserviceindia.com/issues/topic1609-justice-ksputtaswamyretd-vs-union-of-india.html visited on 22nd December 2022 at 02.30pm.

"The right to privacy has been read into Article 21 with the expansive interpretation of the 'personal liberty' by the Supreme Court, but this right is not an absolute right and, if there were conflict between fundamental rights of the two parties,that right which advances the public morality will prevail".

Life Meaning

The expression 'life' in Article 21 has been interpreted by the Supreme Court rather liberally and broadly. "Over time, the Court has been giving an expansive interpretation to 'life'. The court has offices quoted the following observation of FIELD,J., in *Munn* v. *Illinois*[206] an American Case By the term 'Life' as here used something more is meant than mere animal existence. The inhabitation against its deprivation extends to all those limbs and faculties by which life is enjoyed". Bhagwati, J. has observed in Fransis Coralie[207]: " We think that the right to life includes the right to live with human dignity and all that goes along with it, namely, the bare necessaries oflife such as adequate nutrition, clothing and shelter over the head and facilities for reading writing and expression oneself in diverse forms, freely moving about and mixing and coming with fellow human beings."

In *P. Rathinam* v.*Union of India*[208] the Supreme Court has defined life. "The right to live with human dignity and the same does not connote continued drudgery. It takes within its fold some of the graces of civilization which makes life worth living andthat the expanded concept of life would mean the tradition culture and heritage of person concerned". "Another shade of right to life unfold in the inhibition against the deprivation of life extends to all those limits and faculties by which life is enjoyed".

The Supreme Court has stated in *R.M. Malkani* v. *State of Maharashtra*[209] "with reference to Article 21, that the telephonic conversation of an innocent citizen would be protected by courts against wrongful or high handed interference by tapping of the conversation by the police. The protection is not for the guilty against the efforts of the police to vindicate the law".

---

[206] 94 U. S. 113 (1877).
[207] Jain, M. P., Indian Constitution Law, Wadhwa Nagpur, Vth Ed. (Rep) 2008.
[208] AIR 1994 Supreme Court 1844.
[209] AIR 1973 Supreme Court 157.

Personal Liberty

The expression 'personal liberty' used in Article 21 has also been given a liberal interpretation. "It does not mean merely the liberty of the body i.e. freedom from physical restraint or freedom from confinement within the bounds of a prison. In other words, it means not only freedom from arrest or detention, from false imprisonment or wrongful confinement, but means much more than that. The term 'personal liberty is not used in a narrow sense but has been used in Article 21 as a compensations term to include within it all those variety of rights of a person which go to make up the personal liberty of a man.[210] At the outset the term' personal liberty' was interpreted to exclude the rights those mentioned in Article 19 this view was expressed in Kharak Singh[211] that while Article 19(1) dealt with particular species or attributes of that freedom, 'personal liberty' in Article 21 would take in and comprise the residue. This was the projection of 'Gopalan' approach of keeping Article 21 separate from Article 19. Nevertheless, the court gave quite a broad dimension to the term 'personal liberty' used in Article 21".

The court ruled that the term 'personal liberty' is used as a compendious term toinclude within itself all the varieties of rights, which go to make up the 'personal liberties. "For example, the Supreme Court held in Kharak Singh that while night domiciliary visits by the police (involving intrusion into his residence, knocking at his door and disturbing his sleep and ordinary comfort) constitute an infringement of personal liberty of an individual enshrined in Article 21, secret picketing of the house by the police or shadowing of his movements do not fall under Article 21, but under Article 19(1) (d). But the minority view expressed by SUBBA RAO J, adopted a muchwider concept of personal liberty". He observed, "No doubt the expression 'personal liberty' is a comprehensive one and the right to move freely is an attribute of personal liberty, it is said that the freedom to move freely is carved out of personal liberty, and therefore, the expression 'personal liberty' in Article 21 excludes that attribute".

In our view, this is not a correct approached. "Both are independent fundamentalrights, though there is overlapping. There is no question of one being carved out of another. The fundamental right to life and personal liberty have many attributes and some of

[210] A.K Gopalan V. State of Madras, AIR 1950 Supreme Court 27: 1950 SCR 88.
[211] Kharak Singh V. State of U.P, AIR 1963 Supreme Court 1295.

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 active, but that cannot be a complete answer unless the said law satisfies the test laid down must satisfy that both the fundamental rights are not infringed by showing that there is a law that it does not amount to a reasonable restriction within the constitution."

In the *State of West Bengal* v. *Ashok Dey*,[212] course of time the view of SUBBARAO J; has become the accepted view. "The expression, personal liberty in Article 21 of the widest amplitude and it covers a variety of rights which go to constitute the personal liberty of man and some of them have been raised to the status of distinct fundamental rights and given additional protection under Article 19". In *Francis Coralie* v. *Union Territory of Delhi*,[213]"upholding the right of a defence to have interviews with her friends and family members. BHAGWATI, J. held that the personalliberty includes rights to socialise with family members and friends as well as to have interviews with her friends".

In *Satwant Singh* v. *A.P.O*,[214] "the right to travel abroad was held to be an aspect of 'personal liberty' of an individual and therefore person can be deprived of his right to travel expect according to the procedure establishment by law. Since a passport is essential for the enjoyment of that right of that right, denial of a passport amounts to deprivation of personal liberty. Hence, a passport for travel cannot be deniedexcept according to procedure established by law".

"In civil litigation, to decide the question of paternity of a child, no party can be compelled by the court to undergo medical examination or blood group test against his will in the absence of any statutory permission for the purpose. No adverse inference can be drawn against him from his refusal to undergo any such test. Otherwise, it amounts to violation of his personal liberty guaranteed by Article 21"[215].

Right to life and Personal Liberty Different facts

Right to life and personal liberty so broadly inferred by the Supreme Court thatit is now known as Human Rights Jurisprudence. "It folds in its robe almost every aspectof life

[212] AIR 1972 Supreme Court 1660
[213] AIR 1981 Supreme Court 746
[214] AIR 1967 Supreme Court 1836.
[215] Gouttam Kundu v. State of West Bengal, AIR 1993 Supreme Court 229

which makes it worth living. Not only the persons who are free but also the persons who are prisoners are assured certain guarantees by the liberal clarifications ofthis very Article". We can discuss it through different approaches-

Rights of Arrested Persons/Prisoners:

In Case of arresting

The guidelines issued by the Supreme Court in the case of *Joginder Singh* v. *State of U.P.*[216], "emphasized that arrest can cause incalculable harm to a person's reputation and self-esteem. Arrest should be made not merely on suspicion but after a reasonable satisfaction reached after some investigation as to the genuineness and bonafides of the complaint and a reasonable belief as to the person' s complicity and asto need to effect arrest. The arrested person has right to inform his relative or friend about his arrest, place of detention, to consult lawyer etc. The rules emerging from decisions such as Joginder Singh,[217] and *D.K. Basu* v. *State of West Bengal*[218] have beenenacted in Sec.50-A of Cr.P.C."

Fair Trial and Speedy

Fair trial is beneficial both to the accused as well as the society. "A conviction resulting from an unfair trial is contrary to our concept of justice.[219] Right to fair trial ina criminal prosecution is enshrined in Article 21 because the procedure also must be fair. Speedy trial has been recognized by the Supreme Court to be implicit in the spectrum of Article 21. Quick justice is now regarded as sine qua non of Article 21". Supreme Court has observed:

"The concept of speedy trial is red into Article 21. As an essential part of the Fundamental Right to life and liberty guaranteed and preserved under our Constitution. The right to speedy trial begins with the actual restraint imposed by arrest and consequent incarceration and continues at all stages, namely, the stage of investigation, enquiry, trial, appeal, and revision so that any possible prejudice that may result from impermissible and avoidable delay from the time of the commission of the offence till

[216] AIR 1994 Supreme Court 1349
[217] Jain, M. P., Indian Constitution Law, Wadhwa Nagpur, Vth Ed. (Rep) 2008
[218] (1997) 1 Supreme Court Cases 260.
[219] State of Punjab v. Baldev Singh, AIR, 1999 Supreme Court 2378

it consummates into a finality can be arrested."[220]

Hussainara v. *Home Secretary, Bihar*(II),[221] "the Supreme Court has emphasised that financial constraints and priorities in disbursement would not enable the Government to avoid it duty to ensure speedy trial to the accused. Supreme Court lamented, It is a crying shame upon our ad judiciary system which keeps men in jail foryears on end without a trial, The Supreme Court has reiterated in *Abdul Rehman Antuley* v. *R.S. Naik*[222] that there is a right to speedy trial of the case pending against him. But there can be no time limit within which a trial must be completed".

"It is, thus, the obligation of the state or the complainant, as the case may be, to prove with the case with reasonable promptitude." Long pre-trial confinement is also very grievous aspect of the present-day administration of criminal justice. "The poor persons have to languish in prisons waiting trial for their offences.[223] The SupremeCourt has declared that after the ' dynamite' interpretation of Article 21 in Maneka Gandhi[224], there is little doubt that any procedure which keeps such large numbers by people behind bars without trial so long cannot possibly be regarded as 'reasonable,just and fair' so as to be confronting with Article 21".

"It is necessary that enacted by the legislature and as administrated by the countsmust radically change its approach to pre-trial, detention and ensure 'reasonable, just and fair' procedure which has creative connotations after Maneka Gandhi' s cases. The Supreme Court has diagnosed the root cause for long pre-trial incarceration to be the present day unsatisfactory and irrational rules for bail which insist merely on financial security from the accused and their sureties. The court has characterized the system of bail in India as 'antiquated'. It is oppressive and weighted against the poor. The court has made the constructive suggestion to change legal provision for bail so thatthese provisions need no longer based merely financial sureties but, that other factor should also be taken into account so that the poor can get their release from the prison pending their trial".

"Right to appeal, legal aid, hand cuffing of under trials etc. Other issues whichreceived

[220] Kartar Singh v. State of Punjab (1994) 3 Supreme Court Cases 569,638
[221] AIR 1979 Supreme Court 1369.
[222] AIR 1992 Supreme Court 1701.
[223] Law Commission of India, 77th Report on Delay and Arrears in Trial Courts
[224] Ibid

attention of the judiciary & it delivered famous and valuable judgement for issues relating to criminal justice system".[225]

Right against Custodial Violence

Custodial violence is the dirty patch on the robe of criminal justice system. "The incidents of brutal police behaviours towards persons detained on suspicion of having committed crimes is evidence of the mindset of the police based on the borrowed, archaic and outmoded police system which British followed in Ireland and not in their own country i.e. Britain. Describing police torture as 'disastrous to our human rights awareness and humanist constitutional order', the Supreme Court has held the state responsible for remedying the situation. If it is found that the police have ill-treated a detenue, they would be entitled to monetary compensation under Article 21. In spiteof the constitutional and statutory provisions aimed at safeguarding personal liberty andlife of a person" (Art 21 & 22), growing incidence of torture and deaths in police custody has been a disturbing factor. The Court has asserted, "The prevision right guaranteed by Article 21 of the Constitution of India cannot be denied to convicts, undertrials, except according to the procedure established by law by placing such reasonablerestrictions as are permitted by law.[226] The Supreme Court has taken up the matter to award the compensation of custodial violence or death in writs".

Right against Surveillance

The constitution does not grant in specific and express terms any right to privacyas such. "Right to privacy is not enumerated as a fundamental right in the Constitution.However, such a right has been called by the Supreme Court from Article 21 and several other provision of state policy. For the first time, as early as 1963 in *Kharak Singh* v.*State of Uttar Pradesh*[227] a question was raised whether the right to privacy could be implied from the existing Fundamental Rights, such as, Article 19(1)(d), 19(1)(e) and 21". The majority of the judges participating in the decision said of the right to privacythat "our Constitution does not in terms confer any like constitutional guarantee".

On the other hand, the majority opinion SUBBA RAO J. was in favour of inferring the

[225] M. H Hoskot v. State of Maharashtra, AIR 1978 Supreme Court 1548
[226] D.K. Basu v. State of West Bengal, AIR 1997 Supreme Court 610
[227] AIR 1963 Supreme Court 1295

right to privacy from the expression 'Personal Liberty' in Article 21.

"Further, the right to personal liberty takes is not only a right to be free from restrictions placed on his movement, but also free from encroachments on his private life. It is true our constitution does not expressly declare a right to privacy as a fundamental right, but the said right is an essential ingredient of personal liberty. Everydemocratic country satisfies domestic life."

Right to Information and Privacy

Democratic societies undoubtedly have to guarantee the right to access to public information; "it is also true that such society's legal regimes must safeguard the individual's right to privacy. Both these rights are often found at the same 'regulatory level'. It is interesting to note that paradoxically, the right to privacy recognized as a fundamental right by our Supreme Court, has found articulation- by way of a safeguard, though limited, against information disclosure under the Information Act".[328]

Personal Information cannot be disclosed under Right to Information

This Act is in complete sensitization of interest of government as well as interestof individual in respect of right to privacy. "In India, in absence of specific legislation on privacy, privacy right has evolved through the interpretive process. The right to privacy flows from Article 21 of the Constitution. As held in Neera's case[228] that the demand for personal information violates the provision of right to privacy envisaged inArticle 21 of the Constitution. The right to privacy is part of Article 21. The same view was also held in Peoples Union of Civil Liberties case.[229]

The importance of right to privacy has been enshrined in Section 8 (1) (j) of the RTI Act, 2005 that right to privacy cannot be hampered. To achieve this purpose, the Information Act outlines a clear list of matters that cannot be made public. There aretwo types of information seen as exceptions to access: the first usually refers to those matters limited to the state in protection of general public good. The second class of information with State or its agencies is personal data of both citizens and artificial or juristic

[228] Bindu Jindal, "Right to Information v. Right to Privacy",
[229] Peoples Union of Civil Liberties v. Union of India, AIR 1997 SC 568.

entities, like corporations. Individual' s personal data is protected by the laws toaccess to confidentiality and by privacy rights".

In *Nagesh Ganesh Patil S.* v. *Public Information Offices, SBI, Bandra, Mumbai*,[230] "the Central Public Information Officers (CPIO) denied the information toappellant under section 8 (1) (j) of the Right to Information Act 2005, being as personalinformation, causing unwarranted invasion of privacy and it was felt that the informationabout the particulars of the handicapped children proposed by the bank employees as legal heirs for getting family pensions is fiduciary in nature under section 8(1) (e) of the RTI Act".

In *C.P.I. O., Supreme Court of India* v. *Subhash Chandra Agarwal*[231] "SupremeCourt held that the privacy rights, by virtue of section (1) (j) of the RTI Act whenever asserted would prevail. However, that is not always the case, since the public interest element, seeps through that provision. Thus when a member of the public requests personal information about a public servant, such as asset declaration made by him- a distinction must be made between the personal data inherent to the position and those that are not, and therefore affect only his/her private life. This balancing task appears tobe easy: but is in practice, not so, having regard to the dynamics inherent in the conflict.If public access to the personal data containing details, like photographs of public servants, personal particulars is requested the balancing exercise, necessarily dependent and evolving on a case by case basis, would take into account of many factors and would require examination, having regard to circumstances of each case".

In a decision of Delhi High Court,[232] "it observed while interpreting the ambitand scope of right to Information in relation to right to privacy under Art 21 that there is exemption from disclosing the information about sexual disorder by the GeneralSecretary of a NGO, and held that information as to sexual disorder, DNA test betweena Govt. officer and his surrogate mother, name of his mother and surrogate step motheris beyond perception of decency and in fact, an invasion into an- other man' s privacy that is sacrosanct facet of Art 21 of the constitution. Personal information sought that has no nexus with a public activity or interest, cannot be provided".

Here is a recent case in which, giving privilege to the right to privacy, "the Nagpur

[230] RTIR II (2013) 9 (CIC).
[231] 111 (2009) CLT 481.
[232] Paardarshita Public Welfare Foundation v. UOI and ors., AIR 2011 Del. 82.

bench of Bombay High Court ruled that personal information, which serves nopublic interest, can't be disclosed under the Right to Information Act,2005.[233] In the given case, respondent Suresh Kumar Patil has sought personal information of ten employees working in Mahatransco through an application dated June 6, 2011. He demanded confidential documents like annual performance appraisal and job description of these employees. The High Court held that such disclosure is unwarranted. Referring to Sec. 8(1) (j) of the RTI Act, the court observed thatdisclosure of personal information, which has no relation with the larger public interest, causes unnecessary intrusion in the individual' s private realm. 'Unless the central or the state information commissioner finds that such disclosure is justified for larger public interest, no personal information must be supplied with,' the court stated. It alsorelied on an unreported apex court judgment of his year, which held that every individual is entitled to right to privacy and such disclosure without reasonable groundsof public interest, violates the right of the individual. Accordingly, the High Court quashed and set aside the order of state information officer while allowing prayers of the petitioners- public information officer and general manager of Mahatransco".

Details of Bank Accounts and Right to Privacy

In *Ramjethmalani* v. *Union of India*[234] Supreme Court held "That details of bankaccount of individuals, without establishment of prima facie grounds to accuse them ofwrong doing, would be a violation of their rights to privacy. Details of bank accounts can be used by those who want to harass, or otherwise cause damage, to individuals. 'Right to Privacy is an integral part of right to life'. This is a cherished constitutional value and it is important that human beings be allowed domain of freedom that are freeof public scrutiny unless they act in an unlawful manner the notion of fundamental rights, such as a right to privacy as part of right to life is not merely that the state is enjoyed from derogating from them. It also includes the responsibility of the state to uphold them against the actions of others in the society, even in the context of exerciseof fundamental rights by those others".

The right to freedom of speech and expression and right to privacy

[233] See Right to Information Act, Section 8
[234] (2011) 8 Supreme Court Cases 1.

The right to freedom of speech and expression and right to privacy are two sidesof the same coin. "As the freedom of speech and expression is vital for the disseminationof information on the matter of public interest, it is equally important to safeguard the private life of an individual to the extent that it is unrelated to public duties or matters of public interest. Law of privacy endeavours to balance these competing freedoms".

"Article 19 (1)(a) of the constitution of India provides Freedom of Speech and Expression whereby every person has the right to express himself by words, writings, gestures, printing, paintings etc. This thus gives the people the right to know otherwise the purpose of Article 19(1)(a) is lost as if people will not receive information then what would be the purpose of others to give information. Freedom of speech is actually implemented when person giving information actually has someone to be his listener.

Media, both print and electronic, exercise their freedom of speech and expressionguaranteed under the Constitution".

In the case of *ABC* v. *commissioner of Police and others*[235], "the petitioner, on behalf of her minor daughter as her mother and next friend brought petition for breach of the right to privacy and confidentiality, of her daughter under right to life guaranteedunder Art 21 of the constitution of India". In R. Rajagopal Justice B.P. Jeevan Reddy opined, "this is for the reason that once a matter becomes a matter of public record, the right to privacy no longer subsists and it becomes a legitimate subject for comment by press and media among other. We are, however, of the opinion that in the interests of decency (Article19(2)) an exception must be carved out to this rule viz, a female who is the victim of a sexual assault, kidnap, abduction or a like offence shouldnot further be subjected to the indignity of her name and the incident being published in press/ media".[236]

While referring to the norm of journalistic conduct the court stated,

i. The press shall not intrude or invade the privacy of an individual, unlessoutweighed by genuine overriding public interest, not being a prurient or morbid curiosity. "So,

[235] 5 February, 2013 Delhi High Court.

[236] Walters Robert, Data Protection Law "A Comparative Analysis of Asia-Pacific and European Approaches", Springer, 2019.

however, that once a matter becomes a matter of public record, the right to privacy no longer subsists and it becomes a legitimate subject for comment by the Press and the media, among others. Special caution is essentialin reports likely to stigmatise women. Things concerning a person's home, family, religion, health, sexuality, personal life and private affair are covered bythe concept of PRIVACY excepting where any of there, impinges upon the public or private interest."

ii. While reporting crime involving rape, objection or kidnap of women/ females orsexual assault on children, or raising doubts and questions touching the chastity, personal character and privacy of women, the names photographs of the victims or other particulars leading to their identity shall not be published.

iii. The court held that telecast of the video recording of the alleged interview by the petitioner along its transcript reveals blatant violation and disregard of thepetitioner's daughter's right to privacy and confidentially the said telecastdiscloses: "the name of the accused father and his place of work along with his designation- which would not only identify him but also the victim as it is disclosed that the victim is his own daughter; the age of the victim; visual shots of the display board of the colony. Revelation of particulars of such nature and to such extent, are patently sufficient for the disclosure of the identity of the petitioner's daughter" "the respondent[345] has acted in utter disregard anddisrespect of the right of the victim of sexual abuse to privacy, recognized notonly as inherent to the fundamental right to life under Article 21 of the constitution, but also enumerated in the norms of journalistic conduct" court alsoorder for compensation of Rs 5 Lakh.

Limitation on Right to Privacy

"Applying the above propositions, these permitted the newspaper to publish the biography of a confirmed criminal 'so far as it appears from the public records, even without his consent or authorisation.' If the press goes beyond this, it would be invading his privacy. The state its officials cannot restrain the said publication. Their remedy, it any, would arise only after the publication".[237]

In *Sharda* v. *Dharmpal*[238] "It was held that constitutional Right to privacy is notan

[237] Khushwant Singh v. Maneka Gandhi, AIR 2002 De 158
[238] AIR 2003 SC 3450.

absolute right. If there were a conflict between fundamental rights of two parties, that right which advances public morality would prevail. Therefore, order to undergo medical test does not offend Article 21. However, such power has to be exercised only when applicant has strong prima facie case".

Thus, privacy cannot be clearly defined; they are a positive and negative cluster of rights. It has two sides: it acknowledges a right to action, a positive right and it is right to pick the audience in other future rights.

Chapter-5

Right to Privacy under Personal Laws

The further inquiry before is to find out the legal protections to right to privacy.'Privacy' is concerned with a man's dignity and liberty. It is a fundamental human rightguaranteed by international laws. It has been an inalienable and integral part of human life since long. Initially, it had a very narrower scope as such thought to be included only 'right to be let alone'. Later, the increasing maturity levels of the democratic systems, rapid development in science and technology, made its scope wider. Now the right to privacy covers many aspects such as, freedom of thought, control over one's body, identity, solitude in one's home, control over self-information, freedom from surveillance, protection of one's reputation, and freedom from searches etc. The USA is the motherland of right to privacy in present form. Privacy's origin could be traced backto an article written by Warren and Brandy published in 'Harvard Law Review' in 1890,in which the concept of Right to Privacy was discussed for the first time.

The stand for privacy, however, need not be taken as hostility against other individuals, against government, or against society. It is but an assertion by the individual of his inviolate personality."

"The right to privacy is the only Constitutional right with a birthday, the 1890 publication of Samuel Warren and Louis Brandeis's The Right to Privacy in the Harvard Law Review. This initial article, however, dealt with torts, and was in fact inspired not by an Orwellian state but by irritation with paparazzi at the debut of Samuel Warren's daughter and their increasingly portable cameras".[239]

Privacy under Torts

"Tort is a wrongful act or damage (not involving a breach of contract) for whicha civil action can be brought. The Right to Privacy is further encompassed in the field of Torts. This is a branch of law governing actions for damages for injuries to certain kinds of rights like, the rights to personal security, property and reputation. The term'tort' is

[239] 4 Harvard law review 193 (1890).

the French equivalent of the English word 'wrong' and of the Roman law term' delict'. It was introduced in English law by Norman jurists. The word 'tort' is derivedfrom the Latin term tortum or twist and implies conduct which is twisted or tortuous".[240]

The law of torts is fashioned as an instrument for making people adhere to standards of reasonable behaviour respect the rights and interests of one another[241]."This is does by protecting interests by providing for situation when a person whose protected interest is violated can recover compensation for the loss suffered by from the person who has violated the same.[362] By "interest" here is meant aclaim want or desire of a human beings which the human being or group of human beings seeks to satisfy and of which therefore the ordering of human relations in civilized society must take account".[242] The Raw determines what interests need protection and it holds the balance when there is a conflict of protected interest. A protected interest gives rise to a legal right, which in turn gives rise to a corresponding legal duty. Some legal rights are absolute and others are where it is necessary to prove actual damage so constitutes of tort are-

1) There must be a wrongful act committed by a person.
2) The wrongful act must give rise to legal damage and
3) The wrongful act must be of such nature as to give rise to a legal remedy in theform of an action for damages.

In 1960, eminent legal scholar William L. Prosser documented how privacy as a legal concept had come to constitute four distinct torts. That is, a person whose privacy has been invaded could sue the invader for damages. These torts still exist today, and are contoured as four separate branches: Intrusion upon seclusion or solitude or into private affairs".

Common law principles of tort as accepted in Indian law do not provide for a direct action for in vision of Privacy. The law of tort seeks to provide protection by theuse of civil wrongs such as defamation trespass & breach of confidence.

"The tort of Defamation involves the right of every person to have his reputation preserved inviolate. It protects an individual's estimation in the view of the society and its defenses are 'truth' and 'privilege', which protect the competing right of freedom of speech. Essentially, under the law of torts, defamation involves a balance of competing

[240] Ratanlal & Dhiralal, The Law of Torts, (Wadhwa Nagpur, 25th Edition. 2006).
[241] Setalwad, Common Law in India p. 109, as quoted by Ratanlal at p. 12.
[242] Popatlal Gokaldas Shah v. Ahmedabad Municipal Corp. AIR 2003 Guj 44.

interests. The only concession for an action, which involves infringement of right to privacy, would be for reasons of, prevention of crime, disorder, or protection of health and morals or protection of rights and freedom of others. Although privacy violations may be pleaded as many different torts depending on the actual circumstances, the main tort remedies are the privacy torts proposed by Dean Prosser and recognized by both Justices Cortes and Carpio. There are four main privacy torts:

a. Nuisance and trespass under Indian Law of Torts.

b. Defamation.

c. Tort of Passing of.

d. Nervious break down.

Justice Vicente v. Mendoza[243] enjoys repeating that law has two elements: logicand rhetoric. Logic forms the bedrock of our jurisprudence, but it is rhetoric that makes Constitutional Law so potent and so seductive. That is, he cautioned, one must read cases with great care, lest one be ensorcelled by the rhetoric and miss the actual logic."[244]

"There are very few cases in which right to privacy has been recognized as a tort. One of them is Sunkara Satyanarayana v. State of Andhra Pradesh[245]. The questionsof privacy tort of trespass and the violation of constitutional rights were raised. In this case the police opened a 'rowdy sheet' in 1973 recording that he became a thief for wantof money due to lack of parental control and circumstances, and the rowdy sheet was continued though there were no complaints against him. When human right is invaded a citizen has remedies in both public and private law. Public law remedies included prerogative writs as also award of compensation. In private law, the trespass which is an offence under the IPC is also a torts and an action lies for damages by way of a suit".

"The court observed that a citizen could sue the police for damages in civil suit for trespass or seek compensation in public law asserting that Human Rights courts

[243] Supreme Court, 79 PHIL. L. J. 876, 876 (2004).

[244] Oscar Franklin B. Tan in "Articulating The Complete Philippine Right to Privacy in Constitutional and Civil Law: A Tribute To Chief Justice Fernando And Justice Carpio", Complete Philippines Rights"2008 Vol. 82.

[245] (1999) 6 ALT 249.

constituted under the protection of Human Rights Act 1993 would be competent to entertain complaints of violation of the right to privacy and to give relief under criminal law as well as civil law. The court issued a writ of mandamus to close the history sheet, which had been arbitrarily kept alive over 26 years and lift it to petitioner to pursue such other remedies as are available to him under law".[246]

Press and Libel Laws

1925, "the Minnesota Legislature enacted a public nuisance law that permitted judges, sitting without juries, to enjoin publication of newspapers and periodicals that regularly and customarily published materials that were, "obscene, lewd, and lascivious" or "malicious, scandalous and defamatory." The regular daily newspaper inthe state did not oppose the law' s enactment. In 1927, Minnesota court enjoined the publication of the Statutory Press, a small weekly Minneapolis newspaper, on the grounds that it had published malicious, scandalous, and defamatory material about thepolice chief, mayor, country attorney, and others. The injunction applied to all future issues of the newspaper. After the Minnesota Supreme Court upheld the law's constitutionality, Jay M. Near, the Statutory Press' s editor, appealed to the Supreme Court".[247]

Speaking through Chief Justice Hughes delivering decision in Near v. MinnesotaEx Rel. Olson[388] the United States Supreme Court delivered;
"This statute, for the suppression as a public nuisance of a newspaper or periodical, is unusual, if not unique, and raises questions of grave importance transcending the local interests involved in the particular action. It is no longer open to doubt that the liberty of press and of speech is within the liberty safeguarded by the due process clause of the Fourteenth Amendment from invasion by state action."

The law of defamation, assumed after the invention of printing, a good deal of importance, which has been considerably enhanced in modern times by the swift development of journalism. The invention of broadcasting by wireless has by extending the area of dissemination of the spoken word added to its power just as the invention of printing did in the case of the written words centuries ago. The advent of television,

[246] Iyer's, Ramaswamy, The Law of Torts, (Lexis Nexis Butterworths, New Delhi. 10th Edition 2007.
[247]William Cohen and David J. Danelski, Constitutional Law: Civil Liberty and Individual Rights,(New York Foundation Press, IV ed., 1997).

internet and 24 hours' news channel on TV and radio, has multiplied that power. The aim of the law in modern condition is not merely to prevent breaches of peace but also to make people adhere to standards of speech and writing which will preserve social order and harmony and make public life and cooperative efforts possible. For many modern types of defamation, the action for damages is more suitable remedy than a criminal prosecution.

Defamation under Indian Law of Torts

Every man has a right to have his reputation preserved inviolate. This right to reputation is acknowledged as an interest personal right of every person as part of the right of personal security.[248] It is a 'jus in rem' a right good against the entire world. A man's reputation is his property more valuable than other property.[249] The law of defamation like many other branches of the law of torts provides for balancing of interests. The competing interest which has to be balanced against the interest which a person has in his reputation is the interest which every person has in freedom of speech.The wrong of defamation protects reputation and defenses to the wrong, viz, truth and privilege protect the freedom of speech. The existing law relating to defamation is a reasonable restriction. The fundamental right of freedom of speech and expression conferred by Article 19(1) (a) of the Indian Constitution and is saved by clause (2) of Article 19.[250]

The wrong of defamation may be committed either by way of writing, or its equipment, or by way of speech. The term libel is used for the former kind of utterances'Slander' for the later. Libel is written & slander is a spoken defamation. In a case,[251] itwas held that bridegroom and his father in refusing to take the bride to their home aftermarriage in full gaze of the guests committed the tort of defamation and damages couldbe awarded for loss of reputation. In this court leaned judge held that they may be a hybrid type of defamation. A defamatory statement is a statement calculated to expose a person to hatred contempt or ridicule or to injure him in his trade business professioncalling or office or to cause him to be shunned or avoided in society. A Libel is a publication of a false and defamatory statement tending to injure the reputation of another person

[248] Blackstone' s Commentary of the Laws of England, Vol I (4th Edition).
[249] Dixon v. Hoden, (1869) LR 7 Eq 488.
[250] Seervai,H.M, Constitutional Law of India (3rd Edition Volume I).
[251] Noor Mohd. v. Mohd. Jiauddin AIR 1992 MP 244.

without lawful justification or excuse. The statement must be expressed in some permanent form e.g. writing, printing, pictures, statue, waxwork effigy etc. A slander is a false and defamatory statement by spoken words or gestures tending to injure the reputation of another[252]. Injury to reputation amounts to violation of person's right to personality and privacy. Following ingredients must be proved to establish Libel-

1) Statement complained of is false.
2) It is in writing.
3) It is published and
4) It is defamatory.

In the civil action for defamation, falsity of the statement must be proved andtruth is the complete defense to the defendant. The test to defamation is whether the words would tend to lower the plaintiff in the estimation right-thinking members of society generally. The plaintiff must show that the defamatory statement refers to him. Sometimes words prima facie innocent may be actionable if their lateral meaning is defamation. Defamation of diseased person is actionable if his defamation affects the reputation of his living near relatives. Publication of defamatory statement is must for the action of defamation. It means the third person comes to know about such statement.A person cannot excuse himself on the ground that he published the Libel by accident or mistake with an honest belief in its truth".[253]

Common Law under Defamation

Slander-

As in case of a Libel, it must be proved that the words complained of are-

(i) False
(i) Published
(ii) Defamatory and
(iv) Special damages Indian Law

The common law rule that slander is not actionable perse has not been followedin India except in a few decisions. Both Libel and Slander are criminal offences under Section 499 of the Penal Code and[254] both are actionable in civil court without proof ofspecial

[252] Ratanlal & Dhiralal, The Law of Torts, (Wadhwa Nagpur, 25th Edition. 2006).

[253] Cassidy v. Daily Mirror Newspaper Ltd, (1929) 2 KB 231: 141 LT 404.

[254] Defamation-Whoever by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or

damage.

In a case,[255] Calcutta H.C. held that imputing unchastely was actionable withoutproof of special damage and further that it was also actionable at the suit of the husbandas the imputation involved that the husband at the food cooked by an unchaste woman and had therefore lost his caste.

Defenses

These are the defenses available in case of defamation-

(ii) Justification by truth

(i) Fair & bonafide comment

(ii) Privilege

Privilege mean that a person stands in such relation to the facts of the case that he is justified in saying or writing that would be slanderous or libelous in anyoneelse.

a. Absolute- A statement is absolute privileged when no action lies for it eventhough it is false and defamatory and made with express malice. On certain occasions the interests of society require that a man should speak out his mind fully and frankly without thought or fear of consequences for e.g. Parliamentary Proceedings, Judicial Proceedings, Military/Naval Proceedings, State Proceedings.
b. Qualified- A statement is said to have a qualified privilege when no action lies for it even though it is false and defamatory unless the plaintiff proves express malice. For e.g. communications made in the course of legal, social or moral duty; for self-protection; for protection of common interest; for public good and; parliamentary reports judicial proceedings and proceedingsat public meetings. Communications made in cases of confidential relationship also come under qualified privilege. For e.g. relationship between husband & wife, father and son, guardian and ward, master and servant, principal and agent, Solicitor and client, partner or even intimate friends.

Remedy for Defamation

knowingor having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter excepted, to defame that person.

Explanation 1.-It may amount to defamation to impute anything to a deceased person, if the imputation would harm the reputation of that person if living, and is intended to be hurtful to the fellings of his familyor other near relatives.

[255] Suxam Teli v. Bipal Teli, (1905) 4 CLJ 388.

As to the remedies for defamation a suit for damages may be brought. The publication of defamatory statement may be restrained by injunction either under Section 38 or 39 of the Specific Relief Act, 1963. The person aggrieved may file a suit for damages. The courts can grant the exemplary damages also when the award of compensatory damages is not itself though sufficient to punish the defendant and to deter him. There can be aggravation or mitigation of damages depending upon facts & circumstances of the case.[256]

"The court has jurisdiction to interfere on an interlocutory application to restrain the publication of a libel. But this justification will not in general be exercised unless the applicant satisfies the court that the statement in the document complained of are untrue. The specific Relief Act, 1963, enables the court to grant an injunction to restrain publications of a libel which would be an offence under the penal code even though it may not be injurious to Plaintiff is person or property".[257]

Privacy under Criminal Laws:

Criminal libel

"The privacy may be invaded of a person by unauthorized publication of facts about that person which are embarrassing. The most crimes are also torts. But the most conspicuous illustration of this is afforded by the defamatory or private libel. It is a crime which not only is a tort, but is constantly treated as such in actual practice. For it is only a misdemeanor and accordingly not affected by the rule which delayed and therefore, usually frustrated civil proceedings for crimes that were of the degree of felonies. Again, it is a crime which, unlike most others, is often committed by persons whose pecuniary means one large enough to enable them to pay whatever compensation a civil court may award. Hence Libels are much more frequently followed up by civil than by criminal proceedings".

"There are the fundamental principles constituting civil and the criminal law of libel-

1) Anyone who publishes a defamatory document concerning another person, so asto tend to bring him into hatred.

[256] K. V. Ramaniah v. Special Public Prosecutor, AIR 1961 AP 190.
[257] Quartz Hill Con. Mining Co. v. Beall, (1882) 20 Ch. D 501

2) The publication need not to be malicious.
3) The unlawful meaning which the document is alleged to have conveyed must beone which it was reasonably capable of conveying to ordinary people of the class addressed.
4) There are certain qualified and absolute privileges.

Under criminal law[258], the defamation has been made a crime. The following are the essential of the offence-

1. The making or publishing of an imputation concerning any person;
2. The means of such imputation are words, writings, signs or visiblerepresentations.
3. Such imputation must have been made with the intention of harming thereputation of the person about whom the imputation is published.

In this way, the reputation of a person which he possesses in the eyes of society, law rightly protects this external esteem of a person in society. There are certain exceptions to defamation.

Imputation of truth for public good; public conduct of public servants; public conduct of public men; comment on cases and conduct of witnesses etc, merits of judicial proceedings, merits of public performances, censure in good faith by person inauthority and complaints to authority".

In "Sewakram Sobhani v. R.K. Karanjiya[259] a majority of judges in the SupremeCourt approved the principle that journalist do not enjoy any special privilege with regard to the publication of news items in newspaper even under act 19 (1) (a) of the constitution. The matter pertaining to the publication of a news item in the 'Blits' as alsoa government report regarding illicit sexual relation between the complainant and a married lady".

In "Mukund Martand Chitis v. Madhuri Chitnis[260] there was a question before the court whether the husband can defame wife. Liberal view was taken by the High Court that was confirmed by Supreme Court that, "But for the serious view taken by theHigh Court the woman would not have been able to indicate her honour and receive compensation for the defamatory statements. In this case, on the wedding night itself, the husband had suspected the chastity of his wife. The bitterness that soon enveloped the couple was such that there were allegations and counter allegations between the two, who separated

[258] Sections. 499 - 502 of The Indian Penal Code 1860.
[259] 1981 Cri. L. J. 894.
[260] AIR 1992 Supreme Court 1804.

within a month. A complaint of theft was lodged against the wife resulting in the search of her house for gold ornaments allegedly stolen by her. Two cases of defamation came to be filed against the husband, in which the accused husbandwas acquitted by the trail court. However, the High Court on appeal set aside the acquittal and sentenced the husband to two months' rigorous imprisonment and fine ofRs 2,000. In the Supreme Court a compromise was reached by which the husband agreedto pay the complainant Rs. 1 lakh along with unqualified apologies".

Right to Private defence and Privacy

"The right to private defence of person and property is recognized in every system of law and the extent of the right varies in inverse ratio to the capacity of the state to protect the life and property of the subject. The reason is obvious. This duty is primarily the duty of the state but no state, no matter how large its resources, can affordto depute a policeman to dog the steps of every bud mash in the country or to be presentat every riot or affray. This necessary limitation on the resources of the state has given to the subject protanto the right to take the law into his own hands and to provide for his own safety".

"The right is a right of defense both of person and property, not necessarily of one' s own person and property, but also of the person and property of others. The rightto private defense is based on the cardinal principle that it is the primary duty of a man to help himself.[261] Bentham in his Principle of Penal Laws say, the right of defenseis absolutely necessary. The vigilance of Magistrate can never make up for the vigilanceof each individual on his own behalf. The fear of the law can never restrain bad men asthe fear of the sum total of individual resistance. Take away this right and you become in so doing the accomplice of all bad men. The right to private defense may extent to cause death"[262].

Sexual Offences and Privacy:

"Sexual autonomy of a lady is the guarantee of freedom of soul and body of her.Sexual offences against women are a trauma to victim and a stag on the fabric of the society. Daily reports and news of sexual assaults are occupying the enhanced space inthe news

[261] Gour, H. S; "Penal Law of India", (Vol I, 11 t h Edition, (Rev. Ed.) 2003).
[262] Section 100 and 103 of Indian Penal Code 1860.

world. The cases like Delhi rape case. Made the legislature to tighten the nooseof law against sex offenders".

Rape-

The word 'rape' is derived from the Latin term 'rapio' which means to seize. "Thus, rape literally means a forcible seizure and that is the essential characteristic feature of the offence.[263] In common parlance, it means intercourse with a woman without her consent by force, fear or fraud. In other words, rape is violation with violence of the private person of a woman, it is an outrage by all canons.[264] Remarkable changes have been made to the law on sexual offences by the criminal law(amendment) Act 2013. The definition of rape has been made very wide. Not onlyhas this age for consent been made from 16 years to 18 years. According to Explanationof Section 375 consent means an unequivocal voluntary agreement which the woman expresses verbally or through no-verbal communication about willingness to participatein the specific sexual act as well as it she does not physically resist the act, it will not amount to consent. Another changes brought forth are the punishment has been rigorousimprisonment. Rapes, committed by Army personnel in the area deployed[265] or by a relative; guardian, teacher or a person in relation of trust;[266] during communal or sectarian violence[267]; on women not able to give consent, below, the age of 16 years, with women suffering from mental or physical disability, causing grievousbodily harm or endangering life, repeatedly on the same woman are made subject to enhanced punished that shall not be less than ten years which may extent to the imprisonment for remainder of the life of the accused and shall also be made liable tofine. The amended laws also specify the enhanced punishment in case of death or resulting in persistent vegetative state of victim. Gang rape has given special mentionunder section 376 D of the Act. Repeat offender under section 376 or sec. 376 A or 376 D. are made subject to life imprisonment or with death".[268]

This Act also provides for compensation in addition to fine under the new sections 375B

[263] Vij, Krishan, "Forensic Medicine and Toxicology", Elsevier, 4th Edition, (2008).

[264] Paul Singh v. State of Haryana AIR 1980 Supreme Court 249.

[265] Indian Penal Code 1860, Section 376(2)(C): - being a member of the armed forces deployed in an area by the Central Government or a State Government commits rape in such area.

[266] Indian Penal Code 1860, Section 376(2)(f): - being a relative, guardian or teacher of, or a person in a position of trust or authority towards the woman, commits rape on such woman.

[267] Indian Penal Code 1860, Section 376(2)(g): - commits rape during communal or sectarian violence

[268] Misra, S.N, "Indian Penal Code", Central Law Publications, Twenty First Edition, (2018).

and 357C of the code of criminal procedure. The State Government shall pay the compensation. The law also provides for the compulsory immediate medical treatment of such victims in any public or private hospital. The hospitals shall also be under the liability to inform the police immediately"[269].

Sexual Harassment

"Sexual Harassment define as uninvited and unwelcome verbal or physicalbehavior of a sexual nature especially by a person in authority to ward a subordinate. Every incident of sexual harassment of a woman is violation of her right to life, personal liberty, gender equality and privacy. The new amendment to Indian Penal Codeadds new crimes to the original Sec. 354[270].Sexual harassment, Assault to disrobe, Voyeurism, Stalking are made as specific crimes. Assault on women to outrage hermodesty under section 354 of Indian Penal Code & Insulting Modesty of woman has now been made subject to extended punishment[271].

Insertion of crimes as sexual harassment Voyeurism and stalking[441] are the welcome step of the legislature to give respect & secure the dignity, autonomy and privacy of a woman over her person".

The Constitution of India (1950) has enshrined the law relating to privacy being a fundamental right as per Article 21. However, the interpretation to Article 21 is not considered to be sufficient to provide complete protection to the data of the Citizens. Picture No. 1 shows the amount of Data that has been utilized by Indian people in the year 2020.

The Information Technology Act 2000 (hence referred to as the IT Act) currently lists the most comprehensive statutory statute which regulates online privacy on the internet. It contains provisions relating to privacy issues in computer system and further contains some of the major provisions which provides for data protection.

[269] Section 357C – Treatment of victims (Criminal Law (Amendment) Act, 2013).
[270] Assault or criminal force to woman with intent to outrage her modesty.
[271] Vishaka vs. State of Rajasthan, AIR 1997 Supreme Court 3011.

Provisions as per the IT Act (2000): [272]

- Section 43: Section 43gives certain penalty for damage to Computer or Computer System's unauthorized access. (download or extract or copy or adding viruses or damaging any Computer System)

- Section 43-45 of the IT Act talks about cyber contravention which has punishment to pay damages by way of compensation (penalty up to one crore rupees).

- Section 43A: Section 43Agives protection against anybody corporate, who failed to possess the sensitive personal data and were negligent in implementing reasonable practices. So, such corporate body shall be liable for penalty (to the aggrieved).

- Section 65: Section 65 gives that if anyone alters with Computer source documents shall be put for imprisonment / fine.

- Section 66: Section 66 provides protection against various kinds of cyber offences such as hacking, identity theft, cheating by personating, breaching piracy and many more.

Under Law of Contract

- Companies are, nowadays, reliant on contract law to secure their information efficiently. Different companies agree with fellow companies, partners and customers to safeguard their information.

- Agreements like "Click wrap Agreement," the "Shrink Wrap Agreement," the "User Licence Agreement," etc, containing provisions related to the dispute arbitration, secrecy and privacy, etc.

- Various Organizations have implemented security policies and standards procedures such as BS 7799 (British standard i.e., BS 7799) and the ISO 17799 standards.

[272] Information Technology Act (2000) (Retrieved 9 June 2022, from: https://www.meity.gov.in/content/information-technology-act-2000-0.

The Indian Penal Code (Herein after referred to as 'IPC')

- It imposes punishment for the online offences mentioned under the provisions like Section 124 (A), Section 153 (A), Section 292, and Section 499 and so on. As per IPC, liability for breaches of data privacy shall be inferred from interconnected crimes.

- In May, 2021, the two-judge Bench at the Hon'ble Supreme Court held that in the case of offences such as Hacking, Data Theft, the IT Act and IPC (1860) would further be attracted. (IT Act must not exclude an effective application of the IPC) [273]

The Personal Data Protection Bill, 2019[130]

In the K.S. Puttaswamy case Justice, the citizen has taken significant efforts while at the same time offering a person's right to privacy that is a basic right. (2019)(herein after referred to as 'PDP Bill'), provides a comprehensive law to safeguard different kinds of data. The major provisions of the PDP Bill are dealt in Chapter IV.

Implications of Justice K.S.Puttaswamy Judgement:

1) Concerns relating to Privacy against State or Non-State Actors:

   It was observed by the Hon'ble 9 Judge Bench of the Hon'ble Supreme Court that the claim of privacy protection can be against State and/or Non- State actors.

2) Informational Privacy:

   Every person has a right to have a control over the data and such person is unable to have a control over their own online presence. If there is an unauthorized use

[273] Jain, M. "Hacking, Data Theft Attract Offences Under IPC Also, Not Just Information Technology Act: Supreme Court", (2021)(Retrieved 10 June 2022, from https://www.livelaw.in/top-stories/supreme-courthacking-and-data-theft-case-information-technologyitact-indian-penal-codeipc-174560) .

of such information, it shall amount to violation of such right.

3) Privacy is a Natural Right:

Privacy is considered to be natural right but such natural right has some specific restrictions which are imposed by States while passing certain tests as mentioned hereunder:

- Such State action shall have a legal mandate;
- Such State action shall be pursuing a 'legitimate state purpose'; and
- Such State action shall be 'proportionate'.

Privacy under Matrimonial Rights

The right to privacy has an important role to play in the area of matrimonial life."In this respect there is need to strike a balance between the individual's decision to marry and procreate children and the permissible limits in the society as an institution. Although the international standard of the right provides for the individual right to marryit has been hard to guarantee this right in any Constitution in view of the social factor, on the one hand, and in view of the other conflicting rights, on the other hand. The right to procreation of children as a part of the right to privacy is another controversial area which cannot be possibly allowed to operate in view of the higher national goal of population-control. The relevant provisions in the Constitution and other laws are discussed here".

"Family is the lowest unit of the society and for the existence of society the existence of family is a must. The free consent of the parties is essential for entering intomarriage relationship. Article 16 of the Universal Declaration of Human Rights, 1948 recognizes the right to marry[274]. Similarly, Article 23 of the International Covenant on Civil and Political Rights, 1966 provides for the protection of family by the society andthe state. It also recognises the equality of the rights of the spouses. Further, Article 12 of the European Convention for the Protection of Human Rights and FundamentalFreedoms,

[274] Article 16 of the Universal Declaration of Human Rights.

1950 states":

"Men and woman of marriageable age have the right to marry and to found a family,according to the national laws governing the exercise of this right".

"Article 17 of the American Convention on the Human Rights, 1969 more elaborately summarizes the right to marry and provides:

1) The family is the natural and fundamental group unit of society and is entitled to protection by society and the state.
2) The right of men and women of marriageable age to marry and to raise a family shall be recognised, if they meet the conditions required by domestic laws, in sofar as such conditions do not affect the principle of non-indiscrimination established in this Convention.
3) No marriage shall be entered into without free and full consent of the intending spouses.
4) The State parties shall take appropriate steps to ensure the equality of rights andthe adequate balancing of responsibilities of the spouses as to marriage, during marriage, and in the event of its dissolution. In case of dissolution, provisions shall be made for the necessary protection of any children solely on the basis oftheir own best interests.
5) The law shall recognise equal rights for children born out of wedlock and thoseborn in wedlock.

Thus states can neither decline to recognise, in principle, a right to marriage as a formal institution with legal effects, nor can they introduce regulations which make these rights illusory for large groups. Legal restrictions on marriage must be conditionedby special and relevant circumstances. The usual ones, which aim at upholding monogamy, protecting very young persons against their own immaturity and raising certain obstacles in cases of bad health or blood relationship are, of course, acceptable.[275] Marriage has always been regarded as a central institution in American society. Alongside its strong symbolic meaning to the partners, marriage bestows concrete legal advantages on the couple: tax benefits, standing to recover damages for certain torts committed against the spouses, rights to succession, and insurance benefits,to name a few. Thus, states have recognised the special importance of marriage to society. The

[275] A. H. Robertson (ed.) Privacy and the Human Rights, 1970.

American Supreme Court also has affirmed the special status of marriage.In Grisworld v. Connecticut[276], the Court declared that marriage ‘is an association that promotes a way of life, not causes, a harmony in living, not political faiths; a bilateral loyalty, not commercial or social projects. Yet it is an association for as noble a purposeas any involved in our prior decisions.’ Moreover, in Loving v. Virginia[277] and Zablocki v. Redhail[278], the Court finny established marriage as a 'basic civil right of man' fundamental to our very existence and survival”.

The issue presented in “Loving v. Virginia concerned the validity of the Virginiaanti-miscegenation statutes, the central features of which are the absolute prohibition ofa ‘white person’ marrying any person other than a ‘white person’. A husband, a ‘white person'’ and his wife, a ‘coloured person’ within the meanings given to those terms by a Virginia . statute, both residents of Virginia, were married in the District of Columbia pursuant to its laws, and shortly thereafter returned to Virginia, where upon their plea of guilty, they were sentenced, in a Virginia state court, to one year in jail for violating Virginia's ban on inter-racial marriages. Their motion to vacate the sentences on the ground of unconstitutionally of these statutes was denied by the trial court.

The Virginia Supreme Court of Appeals affirmed. On appeal, the Supreme Courtof the United States reversed the conviction. In an opinion by Warren, Ch. J., expressingthe view of eight members of the court, it was held that the Virginia statutes violated both, the equal protection and the due process clauses of the Fourteenth Amendment. Stewart, J., concurred in the judgment on the ground that a state law making the criminality of an act depend upon the race of the actor is invalid. The Court observed that the freedom to marry is one of the vital personal rights protected by the due processclause of the Fourteenth Amendment as essential to the orderly pursuit of happiness byfree man. Marriage is one of the basic civil rights of man, fundamental to our very existence and survival. The Fourteenth Amendment requires that the freedom of choiceto marry, not be restricted by invidious racial discriminations; the freedom to marry, ornot marry, a person of another race resides with the individual and cannot be infringed by the state”.

[276] 381 U.S. 479 (1965).
[277] 388 U.S. I (1967).
[278] 434 U.S. 374 (1978).

In "Zablocki v. Redhail[279], under the terms of a Wisconsin statute providing thatany resident of Wisconsin having minor issue not in his custody and which he is under an obligation to support by any court order or judgment was not to marry, within Wisconsin or elsewhere, without first obtaining a court's permission to marry which permission could not be granted unless the applicant submitted proof of compliance with the support obligation, and in addition, demonstrated that the children covered by the support order are not then, and are not likely thereafter, to become public charges. A Wisconsin resident, who was under a court order to support his illegitimate child was denied a marriage licence by the county clerk of Milwaukee county on the sole ground that he had not obtained a court order granting him permission to marry. Thereafter, the applicant, who would have been unable to satisfy either of the statutory prerequisites for a court order granting permission to marry, brought a civil rights class action in the United States District Court for the Eastern District of Wisconsin, asserting that the Wisconsin statute violated the United States Constitution. The three judge District Court held that the statute was unconstitutional under the equal protection clause of the Fourteenth Amendment".

The Gramm-leach-Bliley act:[280]

- The Gramm-Leach-Bliley Act (herein after referred to as 'GLBA') seeks to prevent the consumer's personal information that has stored in the financial institutions.
- GLBA basically governs the protection of personal information by Banking/Financial Institutions, or Insurance Companies. It talks about Non-Public Personal Information (herein after referred to as 'NPI'), which consists of any kind of information that a Financial Institution stores from their customers.

[279] 434 U.S. 374 (1978).

[280] Gramm-Leach-Bliley Act (2021)(Retrieved 10 June 2022, from: https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act)

- GLBA provides requirements on Financial Institutions for safeguarding NPI and its usage and further giving alerts to the Customers in the case when NPI is exposed to an individual in an unauthorized manner.

- Further, Financial Institutions are obliged to give yearly notice to their Customers about their own privacy policies and about right to 'optout' to share personal information with 3rd parties.

- To comply with GLBA, financial institutions must provide clear disclosure of:

1) Related Policies concerning NPI disclosure to different Entities;

2) NPI categories stored by any Institution and;

3) Related Policies to safeguard security and confidentiality of NPI.

Children's Online Privacy protection Act:[281]

- The Children's Online Privacy Protection Act (herein after referred to as 'COPPA') was created to prevent the children (below 13 years of age) using the Internet through some regulations as to how websites store or disclose personal information of the children.

- As per the provisions of COPPA, before any website operator stores personal information of children, it shall notify their concerned parent about their practices to collect and store data and it shall collect consent of such parent for the purpose of collecting the child's information.

- COPPA is applicable to website operators which collects children related information (knowingly or otherwise).

Payment Card Industry Data Security Standard (PCI-DSS)

- While following financial legislations and regulation, the big credit card based Companies have need of businesses that collects, transmits or processes data relating to the payment card in order to comply with the PCI-DSS.

[281] Children's Online Privacy Protection Act (2021) (Retrieved 10 June 2021, from: http://euro.ecom.cmu.edu/program/law/08-732/Regulatory/coppa.pdf)

- PCI-DSS is regarded as the security standard for Organizations in order to process/ store/ transport credit card data and information.

- Multiple credit card Organizations participating in PCI-DSS framework are VISA, Master Card, American Express, Discover Card and so on.

- PCI DSS basically, consists a set of twelve different standard requirements to process and protect information of every cardholder.

While having a broad comparison of the Indian legislation on online privacy and data protection with the law of developed Nations such as United Kingdom and USA, the adequate requirement for amending the Indian law can be analyzed. Today, Data does not have the same importance or usage and it may vary from one Nation to other Nation on such basis. US have bunch of laws (like Health Insurance Portability And Accountability Act, The Gramm-Leach-Bliley Act Children's Online Privacy Protection Act, California Consumer Privacy Act and so on) for handling out different categories of Data while United Kingdom has one comprehensive law i.e., GDPR.

Further, IT Act majorly deals with extraction of data, cyber contraventions and cyber offence. However, the Companies cannot get adequate amount of data protection of data from it, so Companies find no other option but to have private contracts to keep their data safe and secured. The PDP Bill, 2019 is going to become an Act in future and it is drafted while comparing it to the GDPR. But it is alleged that the PDP Bill has certain lacunas under it. Therefore, it can be recommended that since US have a compiled legislations in relation to protecting all kinds of Data; such approach might be more favorable in the present times.

While dealing with US Privacy laws, California, who has sufficient economy and population, is considered to be having more restrictive laws as it has around twenty five legislations in consonance with it. So, Californian laws basically put a trend for other US States and other Nations. The scope of CCPA is for some profit-making entities only while excluding relatively smaller entities in order to mandatorily comply with it. Adding to it, the PDP Bill is having a stricter compliance while processing the Individual's Sensitive Personal Data. It can be need of the hour for effectively utilizing the Sensitive Personal Data processing of an Individual in India.

While dealing with European Union's Privacy laws, it has given some stringent regulations and laws in GDPR that can effectively protect the citizen's Personal Data.

GDPR provides strict accountability like hefty fines for any Organization at fault. Such huge fines can set an example for other Companies to comply under GDPR, whenever deemed necessary. So, such law is required in India in order to actually provide right to privacy under Article 21 of the Constitution of India (1950). Lastly, it is hugely demanded that PDP Bill is required to become an Act now.

Chapter-6

Digital Privacy in Indian Perspective

As discussed in previous chapter privacy is an integral part of overall development of a human being. One cannot imagine living life to the fullest extent if he is deprived of his privacy. We are living in an era where State is imposed with the duty to secure welfare of people. Such welfare cannot be guaranteed unless people enjoy their right to privacy. It is duty of every State to secure, those rights of individual, which are necessary for his development and welfare. 'Right to Privacy' is one of them. It is therefore necessary to understand its meaning, nature and scope. Right to privacy is not an isolated right and may be understood differently in different contexts. It may mean right against illegal surveillance or right against publication of personal conversation or personal photographs in public domain etc. In this chapter, the researcher proposes is to study statutory mechanism guarding personal data privacy in India. The effort will be made to explore the regulatory mechanism and its viability for the protection of Right to Privacy. The attempt will be made to test the second hypothesis of this research that whether there is adequate legislative protection to personal data under existing cyber law in India or not.

It may also be understood as protection of information or data privacy. Data privacy is the developing connection between technology and the legal right to privacy in the collecting and exchange of personal data. Data privacy is part of the privacy policy. In this kind of privacy, it is a question of collecting and stored, in digital form, unique identifying information pertaining to a person or people. State is also obliged to safeguard people's privacy. Efforts to preserve the privacy and privacy of the Internet should be made. Internet privacy is here a wide word that refers to the many information, communication and decision-making issues, technologies and tactics designed to be private. It includes the right or requirement for personal privacy in respect of the storage, repurpose, supply and presentation of personal information via the internally[282].

[282] Internet Privacy, available at: http://en.wikipedia.org/wiki/lnternet privacy (Visited on September 12, 2022).

Today, confidentiality has become a major focus. There had been a multiplication of sheer chance incursion into a tight and interconnected society. The more subtle incursions into previously untouched regions and the growing demands of commercial and governmental entities for personal information by more sophisticated scientific instruments have generated a new feeling that privacy has to be defended.[283]

Till date Government of India has taken certain significant steps to protect internet privacy and data privacy of people. This includes enacting of Information Technology Act, 2000 and its allied Rules. But the question is whether these efforts are adequate enough? To scrutinize whether we have adequate legislative mechanism to protect online personal data privacy an analysis of laws governing it becomes more important.

INFORMATION TECHNOLOGY ACT, 2000

Information Technology Act 2000 marks the beginning of legislative efforts made by Government of India to resolve issues arising out of information technology. The Act was basically enacted to supplement e-commerce in India. It covered provision regulating egovernance, recognition of electronic records, cyber offences, and intermediaries. The Act has also made an attempt to protect data privacy of individuals.

Historical background of Information Technology Act, 2000

The Model Law of Electronic Commerce, established by UN Commission on International Trade Law in 1996, was approved by the United Nation General Assembly by Resolution A/RES/51/162 on 30 January 1997. The UNCITRAL e-commerce Model Law is referred to as this. The Model Law one Commerce seeks to assist e-commerce by establishing a set of globally accepted standards to allow the removal of legal barriers and increased legal provision for e-commerce via electronic means.[284]. It recommended that by this resolution States need to give favorable consideration to the

[283] Charles Fried, Privacy The Yale Law Journal, Vol. 77, No. 3 (Ian., 1968), 475-493, The Yale Law journal Company, Inc. Available at, http://www.jstor.org/stable/794941 (Visited on September 12, 2022)
[284] UNC!TRAL Model Law on Electronic Commerce, available at:/http:// www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Moode I. html, (Visited on September 12, 2022).

Model Law on e-Commerce. Earlier in the Report of the United Nations Commission on International Trade Law on the work of its seventeenth session (New York, 25 June- to July 1984) (A/39/17) discussed necessity of formulating uniform rules in respect of e-commerce. For example, it discussed legality of electronic funds transfers and electronic signatures [285] , "Information Technology (Reasonable Security Practices and Procedures Sensitive Personal Data or Information) Rules were enacted."

IT Act, 2000 and Data Privacy Information Technology Act, 2000 is the parent Act regulating information, communication technology issues of digital world in India. There are several hurdles to protect privacy in the era of information technology. One of them is definition itself. Despite numerous attempts to find effective legal measures to protect user online privacy this task has proven to be a formidable challenge. The lack of a holistic definition is one of the explanations for this phenomenon. The reason behind this is that privacy is often used as an "umbrella term" for a variety of meanings and situations [286] . Information Technology Act, 2000 has taken efforts to a certain extent to regulate privacy issues.

Interception of Private Communication through phone tapping

Privacy & interception of private communication, Interception of private communication through phone tapping leads to violation of right to privacy. Indian Telegraph Act regulates the law governing telephone tapping in India. The wire-tapping provision is often referred to as section 5 of the Telegraph Act of 1885. It authorizes the government in the event of a public emergency or for the sake of public safety to take over any authorized telegraphs. It may also order communication to be intercepted in the interest of India's sovereignty and integrity, State security, a cordial relationship with other countries or the public order or for preventing inducement to commit a crime. The government must nonetheless follow the procedures for issuing the order set forth by law. Section 7 of the Telegraph Act of 1885 provides the authority to lay forth

[285] United Nation Commission on Trade Law Year Book of 1984, available at: http://www.uncitral. Org/pdf/English/yearbooks/yb-1984-en/yb_l984_e.pdf (Visited on September 12, 2022).

[286] Hanna Krasnova and Paula Kift, "Online Privacy Concerns and Legal Assurance A User Perspective," available at: http://warhol.wiwi.hu-berlin.de/-hkrasnova/Ongoing_ Research file/ Privacy %20Repor t%20HIG%20Hanna%20 Krasnova%20Paula%20 kift% 20SUBMIS S I 0 N % 2 O W orkshop.pdf (Visited on September 12, 2022).

regulations for telegraph behavior. Privacy rights are a component of Article 21's right to life. Unless due process set by law is followed, the right to life cannot be limited. Therefore, a consistent method to intercept or monitor or decode online information should be developed for interception and power. The Act allows Government to provide instructions on any computer resources for interception or monitoring or decryption of information. It states that where, in the interest of the sovereignty or integrity of India, a central government, State Government, friendly relationship or public order or in order to prevent the commission of a recognisable offence relating to the above mentioned offence, or to investigate any offence of public order is specifically authorised to act for the purpose of the Central Government or of any of its Officers. And if requested by the authorised agency, the subscriber or intermediary, or any person in authority, must provide all the facilities and technical support

Collection of data Without consent

Data privacy is breached if anybody acquires data without consent of the provider of data. An individual may store personal data on a computer and if someone downloads it then it will be a breach of data privacy. Section 43 of the IT Act imposes a penalty for unauthorized downloading of data by introducing computer contaminant or virus into computer or computer system.

Privacy vis-a-vis breach of confidentiality

If a person has legally obtained access, he or she shall not take unfair advantage of any personal, electronic record, book, register or document by revealing the same to other parties without permission from the disclosing party. In this connection, Section 72 of the Information Technology Act allows for penalties for infringement of privacy and secrecy. The section provides that any person who has guaranteed access to electronic documents, books, regists, mailing materials, information, documents or other material in accordance with any of the powers conferred on them under the IT Act, rules or regulations made there under without the consent of the data subject is liable with imprisonment for a term w Such persons may be Certificating Authority Controllers, a

person authorised to exercise his/her powers by the Controller, any government authority to access the protected system or the certification authority's operational officers who received information in accordance with the powers conferred in this Act.

Privacy issues- entity holding Information in trust

Any entity which handles personal information must make it sure that the integrity and security of information should remain intact. If security or integrity is compromised it will directly cause violation of personal data privacy. Article 43A of the IT Act provides compensation for non-compliance with data protection. If an entity that owns, controls, or operates, owns, or handles sensitive information or personal data in a computer resource, fails to implement and maintain sensible safety practices and procedures and thereby causes any person to lose or gain incorrectly, such entity shall be liable to compensation of Rupees 5 crores at the most. It is essential to understand what defines an enterprise to apply this provision effectively. Body Corporate denotes any corporation and includes a company, single owner or any group of people involved in business or trade operations[287].

Disclosure of information in breach of lawful contract

In breach of the legal contract, Section 72A imposes sanctions on the publication of information. It states that any person and intermediary providing services under the legal contract shall be punishes with a prison term for a term extending up to 3 years or a fine extending up to 5 rupees lakh, if he or she ensures access to personal information and intends to lead to unlawful loss and misuse, without consent of any person or intermediary who discloses the same person. An intermediary for any specific electronic record means any person who receives, records or performs any services on behalf of another person with regard to that record and includes those storage or transmissions.

[287] See Sec. 43A (i) of Information Technology Act, 2000.

The information technology (intermediary guidelines and digital media ethics code) rules, 2021[288]

On 25th February, 2021, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (hereinafter referred to as "the Intermediary Rules (2021))", has been notified by the Meit Y and the IB Ministry.

While regulating content under the Over-the-top platforms under the Intermediary Rules (2021), the Central Government has given an official statement that there is a rise in concerns about certain issues in regards to digital contents on Over-the-top platform sand also on digital media.

Important provisions under the Intermediary Rules (2021)

- Significant Social Media Intermediary:

  According to Rule 2(v) of the Intermediary Rules (2021), a "Significant Social Media Intermediary" is a social media intermediary that consists of certain number of registered Users within the India that are more than the threshold (such threshold to be notified by the Government of India).

- Social Media Intermediary:

  According to Rule 2(w) of the Intermediary Rules (2021), a "Social Media Intermediary" is an intermediary which directly helps 2 or more Users to interact with each other and permits the both for making, transferring, uploading, altering or accessing any information while utilizing such social media services.

- Due Diligence:

  As a duty, the Significant Social Media Intermediary and also the Social Media Intermediary is required to perform a due diligence. Post receiving an 'actual knowledge' via a Judicial order via an Agency of the Government, the concerned Intermediary is obliged to eradicate such unlawful information under the period of

[288] "The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Ministry of Electronics and Information Technology, Government of India", (2022) (Visited on 22 June 2022, from https://www.meity.gov.in/content/notification-dated-25th-february-2021-gsr-139einformation-technology-intermediary)

36 Hours" as per the Rule 3(1)(d)of the Intermediary Rules (2021).

- Showing Privacy Policy and the details of utilizing Personal Data:

  According to Rule 4 of the Intermediary Rules (2021), it is mandatory for each intermediary for publishing the privacy policy and the use of User's personal data or information, on their respective Applications or Websites or on both platforms.

- Informational Privacy:

  According to Rule 4(2) of the Intermediary Rules (2021), if any Significant Social Media Intermediary is providing messaging services to the Users, then it is mandatory for such Significant Social Media Intermediary to know the 1st Originator's identification of the data on their respective computer resource, as in certain case, be required by a judicial order via a Competent Court or the Competent Authority.

- Information under Unity, Integrity and Sovereignty of the State:

  - According to Rule 4(1) (c) of the Intermediary Rules (2021), any information that breaches the unity, integrity and sovereignty of the state is prohibited.

  - It is mandatory for each Intermediary for providing a notification to the all the Users that if there is any transmission of an unethical information, then it may lead to User's account termination or eradicating such information that does not conform with the Privacy Policy or Agreement with the User.

    - Mechanism relating to Grievance Redressal:

  - The name and contact details of the Grievance Officer along with the mechanism to lodge a complaint against the violation of Rule 4 or any other Rules, is to be mandatorily publish on

    Intermediary's website and/or application by the Intermediary.

- It is mandatory for such Grievance Officer to her such complaints under the period of 3 working days and resolve such complaints under the period of 1 month.

- Removing certain information:

  According to Rule 4(1) (p) of the Intermediary Rules (2021), it is mandatory for Intermediary eradicate Erta in information under the period of 1 day from a complaint which depicts an individual in bad light or exposes such individual's private body parts or depicts such individual in sexual act.

"There may also inadvertently reveal information through his search strings. Retention of that search string would mean that his search engine has a record of his name and Social Security number.8 Major search engines have said they need to retain personal data, in part, to provide better services, to thwart security threats, to keep people from gaming search ranking results, and to combat click fraud scammers". However, major search engines often have retained this data for over a year; seemingly well beyond the time frame necessary to address these concerns. "Some search engines have reduced the time that they retain users' IP addresses. Major search engines delete or anonymize IP addresses according to the following schedule: Yahoo-18 months, Bing (formerly MSN/WindowsLive)-6 months, and Google-9 months[289].

a) Start page: A search engine operated by Ixquick, based in The Netherlands, doesnot record users' IP addresses at all. The privacy policy was created partially inresponse to fears that if the company retained the information, it would eventually be misused. The company concluded, 'If the data is not stored, usersprivacy can't be breached.' Start page will remove all identifying information from your query and submit it anonymously to Google.[290]
b) Online Privacy Tip: It's a good idea to avoid using the same web site for both your web-based email and as your search engine. Web email accounts will always require some type of a login, so if you use the same site as your search engine, your searches can be connected to your email account. By using different web sites for different needs - perhaps Yahoo for your email and Google for yoursearches -- you can help limit the total

[289] https://www.privacyrights.org/print/fs/fs18-cyb.htm. Visited on 29 January 2023 at 05.45pm.
[290] http://www.startpage.com/ Visited 15 March 2023 at 09.21pm.

amount of information retained by any one site.

Alternatively, “log out of your email and clear your browser's cookies before going to other sites, so that your searches and browsing are not connected to your emailaddress. Avoid downloading search engine toolbars (for example, the Google toolbar orYahoo toolbar). Toolbars may permit the collection of information about your web surfing habits. Watch out that you do not inadvertently download a toolbar when downloading software, particularly free software. Google combines information about you from most of its services, including its search engine, Gmail, and YouTube”.

“Hacking has been around for more than a century. In the 1870s in the USA, several teenagers were flung off the country’s brand new phone system by enraged authorities. During early 1960s, university facilities with huge mainframe computers like MIT’s artificial intelligence lab became staging grounds for hackers. In early 1970s,John Draper made a long-distance call for free by blowing a precise tone into a telephonethat tells the phone system to open a line. He was arrested repeatedly for phone tampering throughout the 1970s. Early 1980s saw several cases in the USA related to hacking. Late 1980s, legislations related to hacking, directly or indirectly, were found. In 1990s, technologies for hacking improved and several countries came out with legislation to stop this modem sophisticated menace called ‘hacking’. There are severalcases registered or unregistered related to hacking, in India. Few examples are: Zeetv.com, goznextjob.com etc., and a notorious group of Pakistani hackers called G- Force during 2001 hacked many websites of Indian organisations, for example, Indian science Congress, Asian Age Newspaper, National Research Centre, Agricultural University of Maharashtra, IIM (Ahmedabad), IIT (Chennai), Indian National Information Technical Promotion (New Delhi) etc. Then in 2002, the website of AssamTourism Department was hacked by unknown hackers. Here the hackers replaced mostof the photographs of tourism interest with pornographies. Perhaps, the most shocking instance of hacking in India is, when a 15-year-old American boy, with a strange namet3k-9, hacked into the Mumbai based Bhaba Atomic Research Centre (BARC) computernetwork, soon after the Pokhran nuclear tests, during May 1998. He passed on the information to his friend named ‘Iran Logik’, an 18-year-old immigrant from Serbia, and placed the list of 800 BARC login names and

passwords to a hacker channel. Again,a group of hackers who call themselves 'Armagedon' gained access to an Indian Bio- Medical research facility during 1998 and stolen the test results and internal memos onthe possible effects of nuclear tests on the country's environment and civilian population. So, from individuals to e-commerce Web sites to the Web sites of governmental organisations and their databases may be targets of hackers".[291]

Hacking could result in the violation of an individual's privacy and has been made a punishable offence under the IT Act. "Section 66 of the IT Act that deals with 'hacking', provides:

(i) Whoever with the intent to cause or knowing that he is likely to cause wrongfulloss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility oraffects it injuriously by any means, commits hacking.

(i) Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both[292].

The emphasis for committing 'hacking' under the IT Act is on the effect on the information residing in the computer and any subsequent wrongful loss due to access rather than mere access to a computer itself. Hacking of protected system is punishable under section 70 of the IT Act".

Cyber Breach of Privacy

"With the advent of multichannel television all over the world, and fast spreading internet network, the privacy of an ordinary person is increasingly under threat. Breach of privacy is the kind of cyber tort which affects a common man. Privacy to a large extent signifies the right to be left alone.[293] The first wiretapping cases heard by the supreme court of USA. Cyber stalking may be a direct 'corollary' toviolation of privacy laws on the Internet. There are several situations one may countenance when one deals with privacy laws on the internet. The following may be the key areas of concern when

[291] Dr. R.K. Tenari, P.K. Sastry and K.V. Ravikumar, "Computer Crime and Computer Forensics", Delhi:Select Publishers, 2002.

[292] IPC Section 425 deals with IT Section 66.

[293] Judge Brandeis used the phrase in his dissent in Olmsted v. United States, 227 U. S. 438 (1978).

one comes across privacy related issues.

a. Interception via wiretapping the phone line on the senders end E- mailing may, thus, be conveniently intercepted in such a manner.

b. Disclosure of contents.

c. Disclosure of essential data while registering onto a particular domain such a chatting site, where precautions and registration policies for the surfer are not conveniently out lined. Section 71 of the Information Technology Act 2000, prohibits interception of e-mail during transit. Similarly reading e-mailing during storage on a computer system isalso prohibited by the above section and section 43 of the Act. The recipient of the e- mail is generally free to share the mailing material with anyone provided it is subject tolegal implications of confidentiality."

Chapter - 7

Emerging Issues & Challenges of Privacy in Digital Era

Any illegal activity which involves use of computer or computer network can come within the ambit of cyber-crimes, either as a weapon, objective or tool to perpetuate crimes. Computer, computer network, or activities might be the target of such action. Crime might be against an individual, an institution or a nation in other words. The distinction between regular crime and cybercrimes lies in the worldwide nature of cyber-crimes.

In nature, it reduces the capacity to capture the guilty party and put the guilty party behind the bars. Anyone with a computer and internet connection can do damage and stay anonymous to a distant system or network. The Internet's anonymity is a serious difficulty confronted by police agencies with cybercrime threats. Even traditional crimes like the ft and defamation, obscenity etc a recommitted with the help 0f computers and internet. In this chapter definition of cyber-crime has been discussed, with the different stages in which it is committed. It further discusses various criterion son which cybercrime scan be classified. This chapter aimed to achieve the third objective of the research that whether cybercrime really poses any threat to online personal data privacy of an individual? The chapter will further focus to analyses different types of cyber-crimes, its modus operandi and how they violate individual's privacy besides causing them economic harm. This will inter alia lead to draw the inference about the third hypothesis that whether the online personal data privacy is vulnerable due to cyber-crimes or not.

Due to its wide spread impact and difficulties for combating and regulating criminality in the cyberspace, the legal system has been experiencing it as one of the deadliest natures of criminality. Beside the other issues like jurisdictional problem, fixing the identity of the offender, verification and retrieval of data for evidence, the traditional legal system have some other problems too. Due to the omnipresence of electronic networking across the world and its potential use in every walk of like, the criminality

may upset the regulatory framework quite easily without even getting any trace either of crime or criminal. It is possible to disturb existing set-up within the fraction of seconds. Within a couple of minutes all the data within the server may lose and the transactions corresponding with these computers, the networks associated with it were rendered useless and stopped. The scenario would be more frightening if everybody, from anywhere in the globe, was connected to a computer. So it is likely that some of the server may collapse within a fraction of a few seconds and also the transitions of these servers would stop. Thus, now, the main concern is the globalization of electronic networking and IT, which may extend its influence beyond frontiers.

Therefore, if something in China is wrong, it might harm India's commercial market if an American bank fails due to e-theft or hacking, the Bombay Stock Exchange's share-market index may tumble!! Criminality has the capacity to demonstrate its effects worldwide via electronic networking. Yet another problem of cyber-crime which differentiated it with traditional form of crime is the criminals which are involving in committing cybercrimes. It has been observed that there cent trend of criminality in cyber space revealed that the youngsters, highly qualified, educated and having command over the technology are committing the crimes. Thus, the talented, literate, technocrat sand computer savvy are appeared in the list of criminals. This worsen the problem because traditional policing and investing a ting machinery have experienced to deal with criminals of lower strata of society, their technique suits to the person who is less literate, unqualified and committing the crime in anger, passion, as greed etc.

Therefore, in this chapter attention has been focused upon the revolutionized impact of information technology on crime and criminal behavior, specially, in cyber space. Globalization and trans-national criminality have also shown quantum increase. This has its influence in order to bear in mind the current globalization wave and its effect on crime. Finally, an examination will be conducted on cyber-crime and how the computer and information technology invention has activated it and influenced it.

“Crime means the act punishable at law”. “Crime means the act for which the law prescribes punishment” are preconceived not ions resting in our society Lawless offences are mythic and only horrible or sinful if they are withdrew from legal features. However, a thorough investigation into the term "crime" exposes several concerns.

Basically, a number of common rules may be established which can ideally apply for all crimes and which can be utilized to determine whether or not individual activities are identified as crimes. They correspond to the ideal characteristics of the overall criminal law.

They are in line with the ideal features of the entire criminal legislation. As described above the main components of the broad classification of any crime as politics, specificity, uniformity and penal punishments are deemed to be criminal.

Classification of cyber crimes

Classification of cyber-crimes is based on victims of cybercrimes, nation2l security, role of computers, perpetrators of crime and security etc.

Classification based on victims of cybercrimes

In modern world cyber-crime is wider concept which encompasses variety of crimes committed by the criminals. There are different criterions to classify them. This typology of cyber-crimes is based on the targeted victims of the cyber-crimes.[294]

- Crimes affecting individuals:

This kind is responsible for most cyber-crimes. The victim may be an Internet user or someone who does not use the Internet as such but nevertheless has a negative impact on crime. For example, Cyber stalking après on who regularly browses the Internet is a crime, affecting user of Internet. But a person, whose account in a bank is siphoned off by a hacker by entry to the bank's computer system, may not have anything to do with cyber space as such but still is a victim of a cyber crime. There can be any number of activities that could fall in this category. The major crimes falling under this heading

[294] David L. Carter, Computer Crime Categories: How techno criminal operate?, FBI Law Enforce-ment Bulletin Available at : http//nsi.org/library/compsec/crimrcom.html(Visited on May 16, 2022).

are infringement of privacy, Identity theft and Cyber Stalking.

- Crimes affecting economy:

Economic crimes conducted via cyberspace or through computers are the most hazardous type of cybercrimes. Important cyberspace economic crimes include:

"Hacking or Cracking of Computer systems and networks

Virus and other malicious programs affecting computers

Computer sabotage and Extortion

Theft of Telecommunication Services

Software piracy and other copyright violations

Economic Espionage by business rivals' independent hackers

Money laundering and Tax evasion using Internet and electronic money transfer

Cyber squatting"

- Crimes affecting National security:

These crimes have potential to affect not only society but also nation large. The security and Public International Law implications regulating these types of crimes have become critical. Internet is increasingly being utilized by various terrorist organizations for spreading their ideology and also for coordinating their activities across the globe.

- Racial and other hate propaganda:

Many hate organizations, especially terrorist groups, utilize the Internet to promote their ideology worldwide. The relative anonymity and the easy and widespread reach of the net makes it an ideal forum for these group steeple it. Ku Kluz Klan, White Aryan Resistance, Skin head sand other neo-Nazi organizations in USA, Anti Jews groups in Europe and Muslim extremist groups are some of the groups that have used the Internet for propagating violence and discrimination against their targets groups.

- Child pornography

Child pornography is another content-based illegal activity which has been spreading its tentacles on the Internet. Many additional activities are based on obscene and pornographic materials on the Internet, but this is not usually regarded to be illegal acts and is left to the discretion of the Internet user, although certain countries across the globe deem these actions unlawful as well.

Classification on the basis of role of the computer in cyber crimes

Computer related crimes could be classified into three major categories according to Dr. David L. Carter, Professor in the School of criminal justice as follows;[295]

Computer as the Target

As the usage of personal computers exponentially grew, the crime did not fall far short of its objective. The objective of a computer or data that is located in it is a wide variety of illicit acts. It may be the common robbery of computer parts, or computer break-ins for spying by foreign intelligence officers. Unauthorized computer access may be both physical and virtual. Physical crimes include robbery, incense, etc., with similar criminal features. Waver, Stakes might be substantially greater since computer theft or destruction may cause valuable loss of data at far higher prices than physical loss. But it's the other kind of crime in the cyber world that is more important because of its ramifications. The aim here is not hardware and physical interaction, but instead incorrect information taking or damaging computer information. In order to perform data theft.

Data destruction, this illegal access to computers largely includes the so-called hacking. By bypassing the Security System such as passwords and carry out certain actions that can include just a 'passing-by' process, making slight changes on the website, destroying

[295] David L. Carter, Computer Crime Categories : How techno criminal operate?, FBI Law Enforce- m ent Bulletin Availabl e at: http//nsi.org/library/compsec/crimrcom.html (Visited on June 18, 2022)

the website or stealing passwords and other personal data, or restarting or denying service to the owner, the hacker or unauthorized user may gain input.

- Computer as Tool

In this type of crimes, the computer is used merely tool. The criminal attempt to commit a crime of traditional nature, however, he employs the computer a stool to mitigate his goal. So, using computer or Internet etc., classic crime is perpetrated. In essence, the criminal uses a new code to control the analytical processes of the computer, so assisting the crime or converting legal computer operations for unlawful goals. Computers are not fundamental to the crime, but connected to the illegal conduct, under this type of computer crime. However, computerization also helps to speed up the crime, allows for the processing of higher volumes of information, and makes it harder to detect and track crime.

This category includes fraudulent use of cards and accounts, theft of accrual money, conversion or translation of accounts, telecommunications fraud, and so on. The rising problem of people using cell telephones and then electronically charging other clients is one example of employing a computer as a tool or instrument for crimes. In this situation, the criminals gain mobile billing codes through the use of scanners attached to mobile computers that are tiny parabolic antennas.

If this scanner is active, it captures and saves mobile phone account numbers. When the computational billing codes are captured, the codes are programmed in additional mobile devices easily by connecting the telephones to a computer. Thus, given the knowledge and provision of the legal system concerning traditional crime, conventional crimes committed by means of a computer are simply examined in the conventional way, but since the computer was utilized, the information technology law of 2000, in each case, is read.

- Computer as incidental

Computers for this kind of crime are not important. Crime may occur without the use of a computer, but technology helps to make crime more rapid, allows the processing

of information provided, and makes it harder to detect and track crime. The Internet benefits enable crooks to become sophisticated and reach worldwide. The introduction of the Internet has enhanced their reach and access and thus made the threat much more severe. For instance, pedophiles and child-pornography are nothing new. Through the Internet, innocent youngsters can be attracted by utilizing fake identities with nearly no fear of discovery. Fraud is not a new offence, likewise. However, the usage of the Internet facilitates the fraudster's ability to target the whole globe and to avoid the repercussions. An example of this form of online fraud is the ever again repetitive Bulgarian money laundering scam where suspects from countries like India are forced to pay substantial amount as administrative fees to facilitate the transfer by Nigeria of enormous sums, promised to cut the money generously. The Internet is being used in a wide range of illicit acts, including the sexual assault and unlawful sale of guns.

In most situations, information on money laundering, drug trafficking and many other organized criminal operations can be saved on computers. To circumvent this, criminal activists typically encrypt their own annihilation by limiting access to the data or programming it. I'm merely incidental in all these situations and I have no direct part in the crime.

- Computer as Associate

The new versions of conventional crimes which emerged because of the broad development of computer access and information technology are another kind of crimes which falls within the jurisdiction of cyber crime. The ideal illustration of this sort of crime is software piracy. It is that software piracy occurs simply because a ready market exists because of the enormous number of computers. Technology progress effectively creates new targets for crime in this sort of cybercrime. Some example of this crime includes falsification, copyright breaches, computer theft, audio and video piracy, etc. As the Internet and computers grow in global culture, cyber crimes of this sort are projected to expand dramatically in the future years.

Classification on the basis of the perpetrators of cyber crime:

- Insiders and Outsiders:

Another way of classifying cybercrimes is on the basis of the profile of criminal. Initiators like workers sometimes perpetrate cyber crimes. It might include from the use of the company computer to cause major harm to the system by some unhappy employees for personal purposes. Nearly every firm is confronted with the problem of computer abusers using their time to surf, talk or do other activities, which impact productivity. Typical insider crimes include missing software and parts, inaccurate login, including using the identity and password of other individuals, undermining payroll systems for their own profit, etc.

The most common external hackers are caused by hackers. While it was a pleasant and tough job to start breaking a password and entering another person's computer system, hacking recently increases when there is a more serious crime. Cyber-spion age potential was recognized by intelligence services throughout the world as computer networks are becoming unavoidable for data collecting and administration. Industrial spy with competitors is also on the rise.

- Hackers

A computer hacker, as the oxford Dictionary defines, is a computer enthusiast who gain sun authorized access to a computer or network. But there is more to it than mere enthusiasm and gaining access. Hackers consider themselves something of an elite, though one to which new members are gladly welcome. There is thus a certain ego satisfaction to be had indentifying our self as a hacker. A hacker is a person seeking knowledge and distributing or sharing it with the world, not to profit from it, but to spread awareness and education. Perhaps the premiere resource, internet, in introducing individuals to hacking is.

Crimes related security

Network security has become a key problem with the creation of the internet and its tremendous expansion. Netizens are more exposed to cybercrime because of their anonymity on the Net. Computer systems have been breached often. The public has now become accessible to private sensitive information. In two countries on the network, confidential information may reside. It can live in the form of packets on

physically stored media such as hard disc, hard drive or memory, or in transit via the actual network cable. These two information countries offer potential for assaults by internet users and internet users. Let's talk briefly about some of them;

 Network Packet Sniffers:

By splitting data into segments which are called packets, network computers interact. As these network packets are not encrypted, any programme that can pluck them from the network and process them may process and understand them. A third party may read the network packages and construct a packet sniffer simply. A sniffer packet is a programme that utilizes a promiscuous network adapter card to collect all network packets delivered across a local network. A sniffer can deliver relevant and frequently sensitive information to its consumers like user account names and passwords.

 Password attacks.

Password assaults may be carried by several means, such as Brute force assaults, Trojan Horse Program. I can give user accounts and passwords for spoofing. Continued attempts at user password or account generally relate to assaults. These repeated efforts are known as brute attacks by force.

 Distribution of sensitive internal information to external sources:

The transfer of sensitive data to rivals or others that utilize it to the harm of owners is at the root of these security breaches. While external intruders are able to copy data with password and IP spoof attacks, internal users may place critical data on an external computer or share a network drive with other users. Internet gambling: In India the Information Technology Act does not specifically deal with this aspect.

There are many of online gaming websites. Online gambling is particularly problematic because in several places it is permitted. The proprietors of these websites in their respective countries are therefore legally wise. Legal concerns emerge when a person

who resides in an abroad such as India visits this website.

Example- "the website www.ladbrokes.com permits users to gamble on a variety of sports such as cricket, football, tennis, golf, motor racing, ice hockey, basketball, baseball, darts, snooker, boxing, athletics, ruby, volley ball, motorcycling, etc."

- Morphing:

Morphing manipulates the original image through an unauthorized user or false identity. The images of women were found to be obtained by fraudulent users and reposted/uploaded on many websites again after the alteration by creating false profiles. This amounts to a breach of Sections 43 and 66 of the I.T. Act, 2000. The infringer might also be booked under IPC. In October, the Times of India alerted the authorities about the fact that a beautician in Delhi shared her images with her cell number with a porn webpage.[296]

- Data Theft-Invasion of Privacy

Information or data has become more valuable than material property. Just like theft of movable in real world, these days precious information is stolen in virtual world and when this data is personal it amounts to violation of personal data privacy Theft of data means that an unknown victim robs computer based information for the purpose of breach or confidentiality. Computer users and big companies are increasing worried about data theft.[297] Data may be stolen in more than one manner. Below are some common techniques:

E-commerce: line-commercial activities private information is stolen.

Password cracking: Even if the intruders are not password-protected or if their passwords can readily be deciphered, they can access and obtain valid data.

Eavesdropping: It is possible to intercept and save data sent over unsecure connections.

[296] Debarati Haldar, "Cybercrime against woman," Available at : http://www.cyberlawti mes.co marticles/ 103.html (Visited on 29 January, 2022).

[297] Data Theft Definition Available at: http:// cybercrime.org.za/data-theft/" (Visited on April 14, 2022)

If no encryption technology is utilized, the eavesdropper is likely to lose your password and other secret information.

 Laptop theft

More and more laptop robbery occurs in business companies and important information contained on the laptop is sold to competitors. Carelessness and absence of laptop data encryption might result in significant losses for the company. Speaking of latest technologies which threatens data privacy is, 'Data mining'. It is a technique that refers to the collection of information that is useful to business from massive quantities of data, trends, buyer habits and even personal information to be utilized for sales purposes (or improve service). Taking into account two major kinds of tasks of data mining, the descriptive data mining, aims at describing the basic characteristics of the existing data and predictive data mining where the inference from the original data is to be predicted.

Data mining is mostly based on surveillance technology, and is a possible invasion of the privacy of persons. Data mining concerns of people may best be viewed as the manifestation of an intuitive awareness of the privacy of their users.[298]
offence can be recognized and rescued. The case can be tested by the judge of first class.

 Identity Theft

The precious commodity is personal information. It's not only the key to financial identification, but the identity of yourself online. Identity theft occurs when someone uses personal information of other without his permission like his name or credit card number etc to commit fraud or other crimes for personal gain. It is for the sole goal of taking that person's name or identity in order to conduct transactions or buys, a crime of getting personal and financial information from another individual. The theft of identity is performed in several ways, says Investopedia. Some ID thieves search for

[298] Jason Millar, "Core privacy: A problem for predictive data mining" Available at http://www.idtr ail. Org/ files/I D%20Trail%20Book/9780195372472_kerr_06.pdf (Visited on February 14, 2022).

bank accounts and credit card statement via trash bins; other high-tech tactics entail having access to company systems to steal client names.[299] Once they have the information they are looking for, identity thievescanruina person's credit rating and the standing of other personal information.

Section 66 c of the Information Technology Act imposes a penalty on any other person with a period of imprisonment of a description that may extend to three years and is liable also to be fined for the use of an electronic signature, password or other Unique identifying characteristic. The unknown and baila bleand may be tested by first-class judges. The non identity includes a copy of the electronic signature, a password and any other unique identifying characteristic of the person concerned, which may be misrepresented or fraudulent download. It includes Phishing, Spear Phishing, Denial of service, installation of spyware, cookies etc Object of this section is multi faceted as its trives to protect all e-commerce and e-governance services provided to online users. In the process of obtaining personal or financial information the offender violates privacy of person whose information is obtained.

 Phishing

Lntheera of information technology, data privacy has becomes acrosanct to individual privacy. Technology being dual edged sword can be misused to harm internet privacy. Phishing anon line offence is similar to and is derived from word fishing in real world where off Enders ends mails (hook) to victims (bait) who think it is genuine mail and relies on it. It is a strategy used to get personal information from reputable firms for identity theft by utilizing bogus emails. These legitimate communications are intended to disseminate personal data to recipients, such as account numbers and passwords, credit card details and social security numbers.[300]

Phishing is a fraudulent purchase by disappointing sensitive passwords of personal data by concealing number of credit cards as somebody has been certain that this

[299] Identity Theft ,Available at:http://www.investopedia.com/terms/i/identitytheft.asp (Visited on June 30, 2022).

[300] Russel Kay, Quick study: Phishing, Available at: http://www.cornputerworld. Corn/s/article/89096/Phishing (visited on June 30, 2022).

information truly is needed. It is a financial offence in which a criminal offender presents a real service provider and sends an email to update credit card records disguised as passwords. National association of Software v. Ajay Sood And Ors the Court defined Phishing as cyber crime in that crime, by utilizing computers and the internet as an authentic entity such as banks, to swindle individuals for the extraction of personal sensitive data such password and credit card details, and to misuse them for generating unlawful money. Modus operandi to commit Phishing is that "an email or message is sent to user falsely claiming to be established legitimate enterprise in an attempt to scam the user in to surrendering private information to be used for identity theft. Such email directs the user to fake website where he is asked to share and update his existing account number, passwords, credit card number etc. This information then reaches to off endersandismis used for online shopping; electronically withdraw money from bank accounts etc." For Example:

In 2003 registered users of E-bay website received emails warning them that their accounts will be closed if they do not do not update their information. A link give ninth email took them to fake E-bay website; those who followed the same got tricked.

In year 2006 a worm took over social networking website 'MySpace' and altered links to direct users to wards websites designed to steal login details.

In the US, a young person allegedly sent America Online messages indicating that AOL receivers had been incurred in troubles. In the letter of the perpetrators AOL was used and lawfully linked. When the receiver followed the AOL billing centre link, they were sent to the bogus AOL site, which had personal information and passwords required. This information was utilized for theft of identity. This information might have potentially been sold to interested parties. The privacy of such persons is likewise compromised during the operation of such a crime.

The banking organization stated in 2005 that the ICICI e-mail ID allegedly provided it with fake e-mails. Information was sent to consumers of this financial institution and the culprit was detained after an investigation. The accused has utilized application software to send spam letters with open source code. He used simply the VSN L to spam an email to clients of financial institutions, as there was no spam box for the VSNL email service provider to filter undesired emails.

After spammering customers have got a reply from 120 consumers, 80 of them genuine

and others wrong, since they do not have debit card information when they are e-banked, as required. The email customers felt it had come from the bank when they completed and presented the sensitive material, the material was addressed to the accused. This is because there was a dynamic connection on the opening page (homepage) of the fake site. The dynamic link has been programmed and the information on the form transferred to the web server by handling Internet Explorer during clicking event (where the fake website is hosted).On the laptop now all the information that acquired from the Reliance.com wireless internet connections on your Acer computer (user name, password, transaction password, debit card number and PIN - mama's maiden name).

This offence is documented in accordance with Articles 419, 420, 465, 468 and 471 and Sections 51, 63 and 65 of the Indian Penal Code, 1957, punishing Rs two lacks who the defendant did not think he would be imprisoned for 3 years and fined.[301]

- Techniques of Phishing attacks[302]

Man-in-the-middle attacks: The attacker is between the consumer and the existing Internet applications in this type of attack, which supports all communication across platforms. For HTTP and HTTPS connections, this type of attack is successful. The consumer is connected as if it were the actual site to the assailant's server, while the attacker's server is connected to the actual site. The server then mediates all interactions between customers and online applications – usually in real time.

URL Obfuscation Attacks: The fraudster employs URL concealing technique to make the user follow the URL to the server without users noticing it has been copied by minimal tweaks to URL. The TCP/IP protocol URL Obfuscation uses the untold, unwritten secrets to enable visitors to visit a site they don't want.

XSS (Cross-site Scripting): In the cross-site scripting attacks the application URL or

[301] Cyber Crime Cell, Mumbai: Case of Phishing Mumbai Police2005 Available at: http:// www.cybercellmumbai.com/case-studies/case-of-fishing (Visited on July 23, 2022).

[302] Neeraj Arora, "Phishing scams in India and Legal Provisions," Available at: http://www.neerajaarora. Com/phishing-scams-in-india-and-legal-provisions (Visited on July 23, 2022).

code injection is used on a specific basis, for the website-based URL application or for the in-bedded field of data. These XSS strategies are often from a site that does not check the user's input before they are returned to the client's web browser.

- Phishing scenario in XSS:

- Victim log sin to a website

This type is recently emerged on the scene. The meaning is 'cross sites scripting' where the offender try to mislead the victim by visualizing the similar web-page or by posing the similar information and divert the attention of victim to grab his personal information like passwords, ID, etc. The modality of the attacker can be summarized in following manner-

- "Attacker has spread mines using an XSS vulnerability
- Victim fall up on an XSS mine
- Victim gets a message saying that their session has terminated, and they have to authenticate again
- Victim's user name and password is sent to attacker"

The offence is recognizable and committed pursuant to Section 778 of the IT Act whereas Section 268 of the Indian Penal Code and other criminal sections apply. This offence is not recognizable, rendered or compounded, but without the permission of a Tribunal, before which any magistrate is pending or triable.

India does not have stringent and express law on phishing like that of United States. The State of California enacted the first U.S. lawmaking Internet phishing a criminal offense. It is pert in end to note here that India does not have a separate specific leg is lotion penalizing Phishing activities. Nor does it have provision for recovery of damages for privacy violation. Similarly unlike California's Anti Phishing Law36[303] it does provide security to driver's license records. One of the early criticisms of the law

[303] "California's Anti-Phishing Law of 2005, Available at: http://itl aw.wikia.com /wiki/California% E 2 %80%99s_A nti-Phish ing_Law_of_2005 (Visi ted on July 12, 2022)

was that since the perpetrators are often outside of California, or even outside the United States, it may prove in effective in deterring the phishing, which tends to be farm oreglobalin nature.

- Law against Phishing in India

Certain provisions of Information Technology Act restrict phishing but the question is whether these lawsare sufficient enough to combat Phishing? By deleting or altering information and data electronically from the account of the victim on the bank system, the criminal is fraudulently compromised. This crime is therefore covered under Section 66 of the Information Technology Act, 2000 and penalized.
In section 66 of the IT law, the Computer Related Offences and States shall be penalized with jail for a period of up to three years, or with a fine that may amount to five lakh rupees, if any conduct, whether dishonestly or fraudulently, as set out in section 43 is carried out.

Section66A(c): “Any person who sends any electronic email or email for purposes O via computer equipment or communicating devices, is used to trick the covered email containing a false link to a bank/organization to mislead the addressee or recipient of the origin of such email and thus clearly contains the terms of Section 66A(c) IT Law, 2000,” which states “to deceive or to mislead the address eeorrecipien tab out the origin of such messages.” Explanation to the section states that "Electronic mail" and "Electronic Mail Message" denotes a message or information that has been produced and transferred or received, including attachments to a text, an image, an audio, a visual and any other electronic records that are to be sent with a message. A message or information. Recently Supreme Court declared Section 66 Aasun constitutional and my stery surrounds what answer law in India has for tackling issue of Phishing. The fraudster disguises himself as the genuine banker in the phishing e-mail, using the unique identifying element of the bank or business, such as the Logo, the Mark, etc., and so obviously draws the provisions of Section 66C IT Act 2000 that penalize theft of identity. It states that anyone who uses the electronic signature, password or any other unique identifying feature of another person in fraud or dishonestly shall be punished for a period extending up to three years by the imprisonment of either description and may be liable for a fine that may extend to one lakh of rupees. By using

a phishing e-mail containing the fake web sites of the bank or of the organizations, the fraudsters personally cheat innocent people, so that whosoever, by any communication device or by any computer resource cheats by person, is punished with a prison sentence as well as an offense u/S. 66D."

"The Information Technology Act, 2000 makes penal provisions under the Chapter XI of the Act and further, Section 81 of the IT Act, 2000" containsanon-obstanteclause, i.e. "the provisions of this Act shall have effect not withstanding anything in consistent there with contained in any other law for the time being in force". The non sin embargo clause provides the rules of the IT Act,2000 a higher impact on other acts, including the Indian Penal Code. Under Section 78 of the Information Technology Law, the above criminal provisions of the IT Act 2000 which are attracted by the phishing scam were, however, rendered bailable.

 Vishing-

Voice phishing a new phenomenon is becoming popular among off Enders which is somewhat similar to phishing; only the mode and means of committing it is different. Voicing is a criminal activity of exploiting social engineering through the telephone system for the goal of paying rewards for accessing confidential personal and financial information from the public. Sometimes called "vishing".[304] Information technology Act has to certain extent made provisions to curb phishing through emails and messages but there is need to enact a stronger law that will regulate. Phishing by voice calls. Vishing i.e. voice phishing does come under Information Technology as mobile are considered as electronic devices.

• Online Defamation

It would be a case of defamation if personal information pertaining to someone with intent to impute him is brought in public domain without his consent and bring in gout

[304]Lacour John, "Vishing campaign steals card data from customers of dozens of banks" Available at : http://blog.phis hlabs.com/vishing-campaign-steals-card-data-from-customers-of-dozens-of-banks (Visited on July 12, 2022)

the same was not in the interest of public good. Computer has become tool for defamation of others. Disgruntled employees of a company may bring out information, secret practices of company which would prove defamatory for the company. Section 499 of Indian Penal Code defines defamation as “whoever by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases here in after excepted, to defame that person.”

Section 67 of Information Technology punishes for distributing or communicating indecent material in electronic structure. "It says whoever distributes or communicates or causes to be distributed in the electronic structure, any material which is licentious or bids to the obscene interest or if its impact is, for example, to will in general debase and ruin people who are likely, having respect to every single significant situation, to peruse, see or hear the matter contained or exemplified in it, will be rebuffed on first conviction with detainment of one or the other depiction for a term which may reach out to three years and with fine which may stretch out to five lakh rupees and in case of a second or ensuing conviction with detainment of one or the other portrayal for a term which may reach out to five years and furthermore with fine which may stretch out to ten lakh rupees.

Cyber obscenity

One of the major side effects of cyber revolution is spread of obscenity. Cyber space offers a very high potential scope for pornography, and makes children and women vulnerable to trafficking. Through, India has no specific legislation to tackle this problem, the general criminal law, Information Technology Act 2800 and the recently enacted Protection of children from sexual offences Act, 2012. Due to technical advancement, no updated technical training of police, jurisdictional problems and difficulty in identifying criminals, it is almost impossible to enforce the regulatory mechanism to curb cyber obscenity or cyber porn. Cyber defamation is also the result of expansiveness of Internet.

Pornography and Privacy

The word "pornography" comes from the Greek "pornographos" literally meaning writing about prostitutes.[305] "One of the commonly accepted definitions of 'pornography' in modern times defines it as sexually explicit material (verbal or pictorial) that is primarily designed to produce sexual arousal in viewers.[306] When value judgments are attached to this definition, pornography is perceived as sexually explicit material designed to produce sexual arousal in consumers that is bad in a certain way. There are many approaches to define pornography such as any sexually explicit material that is bad, although a particularly dominant approach has been to define pornography in terms of obscenity. This is also the practice followed in India, where pornography is seen as an aggravated form of obscenity".

"The entire gamut of Indian legislations dealing with obscenity has been upheldas valid under Article 19(2) of the Indian Constitution which allows for the State to impose reasonable restrictions on the Right to freedom of speech and expression on grounds of inter alia public order, decency and morality. The only judicial pronouncement[307] on the issue of the clash between obscenity and freedom of speech and expression recognized that the cherished right on which our democracy rests is meant for the expression of free opinions to change political or social conditions and for the advancement of human knowledge[308]. The Court, however, went on to uphold the validity of Section 292 of the Indian Penal Code[309] on the ground that it manifestly embodies a restriction in the interest of public decency and morality and the law against obscenity, of course, correctly understood and applied, seeks no more than to promote these values".

"This approach by the Legislature as well as the Judiciary has completely failedto demonstrate how private use and enjoyment of pornographic material violates public decency and morality. The theoretical basis for this approach seems to be grounded in

[305] Wolfson, Eroticism, Obscenity, Pornography and Free Speech, 60 Brook. L. Rev. (1994 – 1995)

[306] Stanford Encyclopaedia of Philosophy. Pornography and Censorship, May 5, 2004, available at http://plato.stanford.edu/entries/pornography-censorship/. visited on January 30, 2023.

[307] Ranjit D. Udeshi v. State of Maharashtra, AIR 1965 SC 881, ¶8 (per Hidayatullah, J.): "There is, of course, some difference between obscenity and pornography in that the latter denotes writings, pictures etc. intended to arouse sexual desire while the former may include writings etc. not intended to do so butwhich have that tendency. Both, of course, offend against public decency and morals but pornography isobscenity in a more aggravated form."

[308] Chandrakant Kalyandas v. State of Maharashtra, (1969) 2 SCC 687.

[309] Supra Note 98

the harm principle,[310] but the State has failed to demonstrate what kind of harm, if any, is caused by the private actions of consenting adults in manufacturing and viewing pornography. The State has also failed to demonstrate the inherent immorality of sexual expression and sexual stimulation through pornographic works. As stated previously, pornography, in its limited acceptable meaning, can serve as a positive contribution towards sexual freedom and liberation[311] of individuals, which would ultimately lead to the healthy development of adults in the society. In the absence of any such exposition, the right to moral independence[312] is violated by legislation whose only justification is the pain and disgust experienced by some people when others read or enjoy pornography".

In India, "our Constitution does not contain a specific provision as to privacy butthe right to privacy has been spelt out by our Supreme Court from the provisions of Article 19(1)(a) dealing with freedom of speech and expression, Article 19(1)(d) dealingwith right to freedom of movement and from Article 21, which deals with right to life and liberty."

"The other reason for these legislations abrogating individual freedom and autonomy is their treatment of sexually explicit material, that is, bringing everything under the overarching umbrella of 'obscenity' without differentiating between private and public consumption of such material, as well as the content of such material whichusually ranges from sexual eroticism, obscenity, pornography, violent and demeaning pornography and child pornography. Identifying this difference in degree could very well be the solution to some of the problems highlighted above. To call something obscene, in the standard use of that term, is to condemn that thing as blatantly disgusting.[313] The corresponding term pornographic, on the other hand, is purely descriptive referring to sexually explicit writing and pictures designed entirely and

[310] Stanford Encyclopaedia of Philosophy. Pornography and Censorship, May 5, 2004, available at http://plato.stanford.edu/entries/pornography-censorship/. visited on January 30, 2023.

[311] K.D. Gaur, A Textbook on The Indian Penal Code (2006)

[312] Ronald Dworkin, Is there a Right to Pornography, 1 Oxford J. Legal Stud. (1981) pp.177. "People have a right not to suffer disadvantage in the distribution of social goods and opportunities, including disadvantage in the liberties permitted to them by the criminal law, just on the ground that their officialsor fellow citizens think that their opinions about the right way for them to lead their own lives are ignobleor wrong."

[313] J. Feinberg, Social Philosophy 36 – 54 (1973) as cited in Joel Feinberg, Pornography and the Criminal Law, 40 U. Pitt. L. Rev. 567, 574 (1978 – 1979).

plausibly to induce sexual excitement in the reader or observer. To use the terms 'obscene' and 'pornographic' interchangeably, is to beg the essentially fundamental and controversial question of whether any or all pornographic materials are really obscene. Essentially, whether any given acknowledged bit of pornography is really obscene is a logically open question to be settled by argument and not by a definitional fiat".

"Ideally, two issues should be examined by courts when dealing with the issue of pornography: whether pornography should be construed as speech intending to communicate ideas, and whether the freedom of speech and expression of persons engaging with pornographic material should be weighed against other rights and interests".[314]

"Some jurisdictions like Canada, the US, UK etc. have at least tried to tackle some of these issues through their legal regimes. The US Supreme Court in Miller v. California[315] laid down the 'contemporary community test' to define an obscenity offense, which allowed the state considerable latitude while making laws on obscenity keeping in mind the understanding of the community. Applying this rule, the court[316] held that in the absence of distribution of the obscene material to minors or the obtrusive exposure of it to unwilling adults, the First[317] and the Fourteenth[318] Amendments of the US Constitution prevents the state and federal governments from any attempt to wholly suppress or ban sexually explicit materials merely on the basis of their 'obscene contents'. The concept of 'contemporary community test' was first acknowledged in Indian scenario in the Indian Supreme Court decision, Ajay Goswami v. Union of India.[319] In this case the court held that the test of 'community mores and standards' is outdated in the context of the internet age which has broken down traditional barriers and made publications from across the globe available with a click of the mouse and hence in judging whether a particular work is obscene regard must be had to contemporary mores and standards".

---

[314] Susan M. Easton, The Problem of Pornography (1994)

[315] 38 L Ed 2d 128: 413 US 15 (1972) 413 US 25 (1973)

[316] Billy Jenkins v. State of Georgia, 41 L Ed 2d 642: 418 US 153 (1973).

[317] 1st Amendment, The Constitution of the USA:"Congress shall make no law abridging the freedom of speech or of the press."

[318] 14th Amendment, The Constitution of the USA: "….No state shall make or enforce any law which shall abridge the privileges or immunities of citizens….nor shall any state deprive any person of life, liberty, or property, without due process of law."

[319] (2007) 1 SCC 143.

"Constitutional law can be many things, but most of all it can be an agent of change. Ultimately, it determines the way we organize our lives, socially and politically. It provides us with insights to help us understand and define our society and where it is heading. It is intimately concerned with giving meaning to ourselves and our relations with others.[320] It is hoped that this revolutionary role of constitutional law is kept in mind by courts before making value judgments on certain types of human behaviour and deciding cases in a manner threatening to individual autonomy".

"Symmetric cryptography can also be used to address the integrity and authentication requirements. The steps taken to provide a secure mechanism for creating and passing on the secret key are referred to as 'key management'.[321]

Asymmetric ('Public Key') Cryptography

Whereas symmetric cryptography has existed, at least in primitive forms, for 2,000 years, asymmetric approaches were only invented in the mid-1970s. "Asymmetric cryptography involves two related keys, referred to as a 'key-pair', one of which only the owner knows (the 'private key') and the other which anyone can know (the public key). The advantages of asymmetric cryptography are that:

a) only one party needs to know the private key; and
b) knowledge of the public key by a third party does not compromise the security of data transmissions.[322]

To crack a mere 40- or 56-bit asymmetric key would be trivially simple, becausethere are far fewer sets of keys (or, expressed more technically, the 'key-space' is 228 relatively 'sparse'). It is currently conventional to regard a 1024-bit asymmetric key length as being necessary to provide security".[323]

Applied Public Key Cryptography

---

[320] Patrick Macklem, Constitutional Ideologies, 20 Ottawa L. Rev. 117, 119 (1988).

[321] Bellare, Mihir; Rogaway, Phillip. "Introduction". Introduction to Modern Cryptography,2005,

[322] https://searchsecurity.techtarget.com/definition/asymmetriccryptography#:~:text=Asymmetric%20cryptography%2C%20also%20known%20as,from%20unauthorized%20access%20or%20use.&text=A%2 0private%20key%20%2D%2D%20also,shared%20only%20with%20key's%20initiator. Visited on 12May 2022 at 09.35pm.

[323] Ibid

“Public key cryptography can be applied as a means of addressing each of the requirements for data transmission security identified in the previous section”.[324]

Public Key Cryptography and Message Transmission Security

“The sender encrypts the message, not with their own key, but using the intended recipient's public key. The receiver decrypts using their private key. This is a more secure approach than symmetric cryptography, because the decryption key need never be in the possession of anyone other than the owner. It is much slower, however, and hence symmetric cryptography is more commonly used for protecting the contents of the message from prying eyes”.[325]

Public Key Cryptography and Integrity, Authentication and Non-Repudiation

“The technique can be used to address all of the integrity, authentication and nonrepudiation requirements. Because the technique is somewhat complex, it is explained below in a succession of steps. This process uses a different key-pair from that used for message transmission security. The key-pair used for message-security is owned by the recipient, whereas the key-pair used in this process is owned by the sender. The sender appends to a message a special, agreed segment within the message. He encrypts this segment with his private key. The recipient decrypts this segment using the sender's public key. If the decrypted segment is identical to what the two parties had previously agreed, then the recipient can be sure that the message has been sent by the purported sender, and that the sender cannot credibly deny having sent it. Hence the authentication and non-repudiation requirements are satisfied”.[326]

“This technique can be taken a step further, to address the integrity requirementas well. The additional segment is not pre-agreed. Instead, a 'message digest' is created, by processing the actual message using a special, pre-agreed algorithm (in a similar way to the MAC’ing process used in symmetric cryptography). The sender encrypts this

[324] https://www.tutorialspoint.com/cryptography/public_key_encryption.htm. Visited on 13 May 2022 at 08.45pm.

[325] Stallings, William Cryptography and Network Security: Principles and Practice. Prentice Hall. 3 May 1990.

[326] Daniel J. Bernstein "Protecting communications against forgery" ,44 MSRI Publications. §5: Public-key signatures, 14 November 2022

message digest with his private key, to produce what is called a digital signature (because it performs much the same function as a written signature, although it is much harder to forge). The recipient re-creates the message digest from the message that they receive, uses the sender's public key to decrypt the digital signature that they received appended to the message itself, and compares the two results. If they are identical, then:

a. the contents of the message received must be the same as that which was sent (satisfying the integrity requirement);
b. the message can only have been sent by the purported sender (satisfying the authentication requirement); and
c. the sender cannot credibly deny that they sent it (satisfying the non-repudiation requirement).

"Rest assured that most people do not grasp those ideas the first time that they read them. The second description is of the process whereby all message transmission security risks can be addressed through the application of public key cryptography".[327]

Contemporary Message Transmission Security

In the late 1990s, "the conventional approach to protecting the security of messages during transmission applies a hybrid of symmetric and asymmetric cryptography. Message content security is achieved using a secret key, with key management performed using an asymmetric key-pair. Integrity, authentication and nonrepudiation are achieved using a separate asymmetric key-pair. The purpose of the Secure Electronic Transactions (SET) specification is to provide a means whereby credit-card details can be used over an open network such as the Internet, with a far higher level of fraud-prevention than is available with manual (flick-flack) machines, and even data-capture at point-of-sale. SET is an open, vendor-neutral, non-proprietary,license-free specification for securing on-line transactions."

"It leverages off the existing payment-card infrastructure and card-base. It is a collaborative initiative, spear-headed by Visa and MasterCard, but including other important players such as Microsoft and Netscape. The scheme involves the use of digital signatures based on public key encryption, as a means of authenticating all

[327] Paar, Christof; Pelzl, Jan; Preneel, Bart Understanding Cryptography: A Textbook for Students and Practitioners. Springer.

participants in a card-based payment transaction".[328]

"The operation of SET depends on software that implements a series of protocolsbeing installed in the workstations or servers of four kinds of people and organisations.These are:

c) cardholders;
d) merchants;
e) payment gateways; and
f) certification authorities".

The simplified representation that follows describes the two key elements:

The establishment of the necessary framework

"Each of the participants has to create a key-pair, store the private key in a securemanner, and make the public key available to organisations that seek it. SET envisages a hierarchy of certification authorities (CAs), independent from other CA hierarchies. These are:

(i) a 'root CA' (God) that certifies payment-processing organisations like Visa, MasterCard and AmEx;
(i) a CA run by or for each payment-processing organisation, which certifies its member-institutions / banks / card-issuers; and
(ii) a CA run by each card-issuer that certifies its cardholders.[329]

A cardholder will (quite probably unconsciously) acquire a certificate from the CA of their card-issuer, a copy of which they can provide whenever they make a purchase. Each card-issuer will acquire a certificate from the CA of each payment processing organisation that they use. Each payment-processing organisation will acquire a certificate from the root CA".[330]

The conduct of a payment transaction

[328] Goldreich, Oded. Foundations of Cryptography: Vol. 2. Cambridge university press, 2004
[329] http://www.rogerclarke.com/II/CryptoSecy.html. Visited on 16 May 2022 at 05.24pm.
[330] Burns E. & Christofis I. (1995) 'Certification of Public Keys: Your Electronic Credentials' EDICAST 26 (October/November 1995)

To effect a transaction, “a card-holder invokes software on their workstation thatinitiates the following sequence:

- the card-holder states that he wishes to make a payment;
- the merchant responds;
- the card-holder provides details of the amount to be paid, together with acopy of their certificate;
- the merchant sends to the payment-processing organisation (via the payment gateway or acquirer) a request for authorisation;
- authorisation is handled by existing processes using existing networks;
- the merchant receives authorisation;
- the merchant sends a capture request (to actually commit the transaction);
- the merchant receives confirmation that the transaction has been accepted;
- (ix) the merchant sends the card-holder confirmation that the payment has been accepted.[331]

Since it was announced with much fanfare in 1996, progress in implementing SET has been slow. This is because the scheme is complex, and depends on many participants conforming to the specification. A particular concern is that the scheme contains nothing that manages participants' private keys. It appears that these will needto be stored on participants' workstations and servers, or on additional peripherals installed on workstations and servers to handle a secure token (probably a chip-card)”.[332]

Infrastructure for Digital Signatures

Two conditions need to be satisfied, in order that public-key digital signatures can satisfy message transmission security needs:

Strong security measures protecting each person's private key,

“For a digital signature to be of high quality (i.e. not readily subject to spoofingand repudiation), it needs to be generated using a 'private key* which is held under highly secure conditions by the person concerned. A private key is long. It is impractical

[331] Clarke R., Dempsey G., Ooi C.N. & O'Connor R.F. 'The Technical Feasibility of Regulating Gambling on the Internet', Conference on 'Gambling, Technology & Society: Regulatory Challenges for the 21st
[332] Ibid

for a private key to be memorised in the way that passwords and PINs are meant to be memorised. An appropriate device to support secure storage of a private key is a chip, and the most practical carrier for such a chip at present is a smart-card. Access to the private key stored on a chip needs to be protected in some manner, such that only the owner can use it. One approach is to protect it with a PIN or password; but this provides only a moderate level of security. An emergent approach is for the card itself to refuse access to the private key, except when the card measures some aspect of the holder's physical person, and is satisfied that it corresponds sufficiently closely (using 'fuzzy matching') to the measure pre-stored in the card. Examples of such 'biometrics' include the patterns formed by rods and cones on the retina, and the geometry of the thumb".[333]

"A significant difficulty that has to be addressed, however, is that, because a business entity cannot itself act, it is dependent on the actions of one or more humans acting on its behalf. In addition to the security measures needed in respect of a person'sown digital signature, further measures are needed, in order to reduce the likelihood of error or fraud by one or more persons, involving misapplication of the business entity'sprivate key".[334]

Additional Issues in Public Key Cryptography

"Public key cryptography is relatively new, technically complex, and raises many public policy issues. The generation of pairs of private and public keys because of the nature of the mathematics underlying asymmetric cryptography, the pairs of keysare created as part of the same process. Three main choices exist as to who performs key-generation:

(i) The key-owner: In this case, the private key never travels outside the owner's premises (or better still outside the owners' secure computer, or chip-card); but the owner must have the technical competence to perform the function, and all parties must have grounds to be confident about the quality of the key-generation process (e.g. through audit and certification of software packages or of hardware,such as smart cards);

[333] Chaum D. 'Digital Signatures and Smart Cards', Digicash bv, Amsterdam, at http://www.Digicash.com/publish/digsig/digbig.html. Visited on 21 May 2022 at 10.00pm.

[334] Clarke R. 'The Monster from the Crypt: Impacts and Effects of Digital Money' Proc. Computers, Freedom & Privacy Conference, San Francisco, at http://www.rogerclarke.com/EC/Monster.html. Visited on 25 May 2022 at 10.11pm.

(i) A service organisation of the owner's choice: In this case, the private key has to travel from the service organisation to the owner, and the owner has to trust the service organisation either not to keep a copy, or to keep a copy subject to an appropriately high set of security standards. Once again the quality must be assured (e.g. through audit and certification of service organisations); or

(ii) A specific government agency or agencies: In this case, the private key has to travel; and trust has to exist; and the location of all private keys is known to, andunder the control of, the State. Some form of assurance is needed that the State,and agencies of the State, will not abuse the trust. [335]

This choice of who generates key-pairs is one of the issues at the heart of the cryptography debates of the last few years".

Escrow of Private Keys

Escrow is an "arrangement whereby something is placed on deposit with a trusted party, but may be accessed by third parties under certain conditions. "It was originally used for title deeds for real property, and is used for source-code for softwarepackages. Escrow can also be used for private keys, in which case it is referred to as 'private key escrow', which is commonly shortened to 'key escrow'. There are a numberof conditions under which individuals or organisations may have a legitimate interest ingaining access to the private keys of other parties."[336]

These include:

a) where an organisation seeks access to the private key used by an officer, employee or agent, especially where the person no longer fulfils that role on behalf of the organisation;
b) where an executor acts on behalf of the estate of a deceased individual;
c) where a law enforcement agency seeks access to a private key in order to materially assist in the investigation of a serious crime; and
d) where a national security agency seeks access to a private key in order to materially

[335] http://www.csc.villanova.edu/~mdamian/Past/csc3990fa08/csrs2007/01-pp1-7-MattBlumenthal.pdf. Visited on 14 June 2022 at 12.54am.

[336] https://en.wikipedia.org/wiki/Key_escrow#:~:text=Key%20escrow%20(also%20known%20as,gain%
20access%20to%20those%20keys. Visited on 18 June 2022 at 11.25pm.

assist in the protection of national security.

If, however, security is to be sustained (and, indeed, if privacy is to be protected),any access to escrowed keys would need to be subject to very careful designed and implemented controls, e.g. a prior requirement of legal authority (such as a search warrant), granted by a senior member of the judiciary. If key escrow is implemented, it might be:

a) voluntary;
b) voluntary for individuals but mandatory for corporations;
c) mandatory for all users; or
d) mandatory for dealings with government.And the function might be performed by:
    a) a service organisation of the key-owner's choice;
    b) a service organisation which must be licensed, and which, as a condition of the licence, has to satisfy certain conditions; or
    c) a specified government agency or agencies.

"These choices, and indeed the very question as to whether private key escrow should be implemented, lie at the heart of the cryptography debates of the last few years. It is important that the distinction be appreciated between secure deposit (for the benefit of the key-owner) be distinguished from escrow (for the benefit of a third party). This has become confused during the public debates".[337]

Biometric Enabled National ID Card and Privacy

In the post September 11, 2001 era, "concerns for prevention of terrorism have been raised throughout the world and simultaneously, the proposals for establishment of nationwide unique identity system have also been generated as an effective counter-terrorism measure in order to prevent illegal immigration along with other fraudulent activities. In this respect Smart Card based technologies have been introduced in different countries throughout the world. Telephone Cards, Employee Cards, ATM Cards, SIM Cards of mobile phones etc. are examples of 'Smart Cards'. After the success of these Smart Cards, countries have started to launch the 'Biometric Enabled National ID Cards' in order to prevent terrorism and related activities. At present,

[337] Garfinkel S. 'PGP: Pretty Good Privacy' O'Reilly & Associates, 1995

several countries like Belgium, Greece, Luxemburg, Germany, France, Portugal and Spain have official compulsory national ID cards, but the Nordic Law Countries including Sweden and Common Law Countries like U.S.A., Canada, New Zealand, Australia and Ireland do not have such cards as well as they have historically rejected attempts to create National ID Cards.[338] U.K. has established a system of National ID Cards by enacting the Identity Cards Act, 2006, but due to opposite remarks and criticisms owing to the adverse effects of that system including the loss of Privacy of the Personal Information of individual Card Holders, the Act has been repealed and the system has been destroyed in 2011. These activities show the worldwide negative attitude towards the establishment of a system of National ID Cards".

Problems of National ID Systems: An Estimation

The existing National ID Systems throughout the world have suffered from various problems and thereby have been objected from different sections of the society."In this respect, six specific problems associated with the National ID Schemes are listedbelow:-

a) National ID Systems have failed to meet stated objectives.
b) National ID Systems create more problems.
c) National ID Systems conceal hidden agendas.
d) National ID Systems lead to function creep and discrimination.
e) Privacy risks surrounding National ID Systems.
f) National ID Systems shift the balance of power from the individual to the state".[339]

Threats to Privacy with the Introduction of National ID Systems: ThePractical Implication

Introduction of National ID Systems may create various threats to Individual Right to Privacy. "It has various reasons. Every identity system is made up of a supportregister containing personal information parallel to that on the ID Card. When this information is maintained on a central database, the ID number acts as a common identifier for

[338] Sheetal Asrani-Dann, "The Right to Privacy in the Era of Smart Governance: Concerns raised by the Introduction of Biometric-Enabled National ID Cards in India", Journal of the Indian Law Institute, Vol.47(3), July-September 2005

[339] https://www.christopher-parsons.com/Main/wp-content/uploads/2013/11/2013-National-ID-Card-by-Stealth.pdf Visited on 12 June 2022 at 08.21pm

multiple government agencies. The risks that this poses for Individual Privacy are monumental. Centralized information is centralized power. A national identifier contained in an ID card enables disparate information about a person scattered in different databanks to be easily linked and analysed through data mining techniques. This would allow the entries in one set of data to influence other unrelated parameters. Moreover, multiple-agency access to sensitive data or multiple-use of the ID card greatly increases the potential for misuse of personal information either through corrupt disclosure or lapses in security. Hence, the Right to Privacy of personal information of the individual citizens is seriously threatened".[340]

Effects of Biometric Enabled National ID Cards on Right to Privacy

"The main problem of Biometric Enabled National ID Card System is that, the use of this technology amounts to a wholesale violation of the Right to Privacy which cannot be justified even on the grounds of compelling state interest. Even if one buys into the need for sacrifice Individual Privacy for an overwhelming national interest, theclaims made by the industry and government that biometric technology is an effective means of achieving stated goals in clearly unsustainable, unsubstantiated and at best questionable".

Disadvantages of Biometric Enabled National ID Card System

"A number of studies have pointed out the following disadvantages of Biometric Enabled National ID Card System:-

a. Not everyone can necessarily be enrolled in a given biometric system.
b. Not every legitimate user is necessarily recognised by a biometric system.
c. Not every illegitimate user is necessarily barred by the biometric system".

Aadhaar Card : Biometric Enabled National ID Card of India

"The Biometric Enabled National ID Card System in India is denoted by a unique identification number, called the Aadhaar Number, printed in the National ID Card, called the Aadhaar Card. In order to provide legal support to the Aadhaar Unique

[340] Arora, S. (2008). National e-ID card schemes: A European overview. Information Security Technical Review, 13, 46-53. https://doi.org/10.1016/j.istr.2008.08.002. Visited on 02 June 2022 at 12.27am.

Identification Number System, Indian Parliament has enacted the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016. The basic objective of the Act is to provide for, as good governance, efficient, transparent and targeted delivery of subsidies, benefits and services, the expenditure of which is incurred from the Consolidated Fund of India, to individuals residing in India through assigning of unique identity numbers to such individuals. The Act has established the Unique Identification Authority of India (UIDAI), which has the power to specify the demographic and biometric information that must be collected for registration. It also has the power to issue Aadhaar numbers to residents, perform verifications and to specify the subsidies and services for which Aadhaar will be required".[341]

Aadhaar and Privacy Violation: An Examination of Indian

"Condition The Aadhaar Act, 2016 has created provisions for the protection of personal information kept with the UIDAI and accordingly, UIDAI must ensure the security of identity information including the authentication records. Such information should not be revealed to anyone, even to the Court in totality and can be revealed to the Joint Secretary only in the interest of national security by an order issued from the Central Government. Though the Aadhaar Act has created provisions for protection of personal information of the individual citizens and has prescribed strict punishments forviolation of the provisions thereof, but it has created serious impact on Individual Rightto Privacy and has generated nationwide concern thereof. In the absence of any expressstatute on Right to Privacy, the four corners of this right are not specifically defined in India. As such, there is every chance of loss of Personal information of the individual citizens by going into the wrong hands".

[341] https://economictimes.indiatimes.com/news/politics-and-nation/aadhaar-scheme-does-not-violate-right-to-privacy-says-sc/articleshow/65969846.cms?from=mdr. Visited on 27 June 2022 at 01.42am.

Chapter - 8

Analysis of Digital Personal Data Protection Act, 2023 with respect to Personal Privacy

As discussed in previous chapter privacy is an integral part of overall development of a human being. One cannot imagine living life to the fullest extent if he is deprived of his privacy. We are living in an era where State is imposed with the duty to secure welfare of people. Such welfare cannot be guaranteed unless people enjoy their right to privacy. It is duty of every State to secure, those rights of individual, which are necessary for his development and welfare. 'Right to Privacy' is one of them. It is therefore necessary to understand its meaning, nature and scope. Right to privacy is not an isolated right and may be understood differently in different contexts. It may mean right against illegal surveillance or right against publication of personal conversation or personal photographs in public domain etc. In this chapter, the researcher proposes is to study statutory mechanism guarding personal data privacy in India. The effort will be made to explore the regulatory mechanism and its viability for the protection of Right to Privacy. The attempt will be made to test the second hypothesis of this research that whether there is adequate legislative protection to personal data under existing cyber law in India or not.

It may also be understood as protection of information or data privacy. Data privacy is the developing connection between technology and the legal right to privacy in the collecting and exchange of personal data. Data privacy is part of the privacy policy. In this kind of privacy, it is a question of collecting and stored, in digital form, unique identifying information pertaining to a person or people. State is also obliged to safeguard people's privacy. Efforts to preserve the privacy and privacy of the Internet should be made. Internet privacy is here a wide word that refers to the many information, communication and decision-making issues, technologies and tactics designed to be private. It includes the right or requirement for personal privacy in respect of the storage, repurposal, supply and presentation of personal information via

the internally[342].

Today, confidentiality has become a major focus. There had been a multiplication of sheer chance incursion into a tight and interconnected society. The more subtle incursions into previously untouched regions and the growing demands of commercial and governmental entities for personal information by more sophisticated scientific instruments have generated a new feeling that privacy has to be defended.[343]

Till date Government of India has taken certain significant steps to protect internet privacy and data privacy of people. This includes enacting of Information Technology Act, 2000 and its allied Rules. But the question is whether these efforts are adequate enough? To scrutinize whether we have adequate legislative mechanism to protect online personal data privacy an analysis of laws governing it becomes more important.

Information Technology Act, 2000

Information Technology Act 2000 marks the beginning of legislative efforts made by Government of India to resolve issues arising out of information technology. The Act was basically enacted to supplement e-commerce in India. It covered provision regulating e-governance, recognition of electronic records, cyber offences, and intermediaries. The Act has also made an attempt to protect data privacy of individuals.

Privacy under Information Technology Act of 2000

"Section 43(b) of the IT Act of 2000, affords cursory safeguards against breachesin data protection.[344] The scope of Section 43(b) is limited to the unauthorized downloading, copying or extraction of data from a computer system: essentially unauthorized access and theft of data from computer systems."

[342] Internet Privacy, available at: http://en.wikipedia.org/wiki/lnternet _privacy (Visited on September 12, 2022)

[343] Charles Fried, Privacy The Yale Law Journal, Vol. 77, No. 3 (Ian., 1968), 475-493, The Yale Law journal Company, Inc. Available at, http://www.jstor.org/stable/794941 (Visited on September 12, 2022)

[344] Section 43(b) in The Information Technology Act, 2000:- downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network includinginformation or data held or stored in any removable storage medium

"Section 43(b) is limited in scope, and fails to meet the breadth and depth of protection that the E.U. Directive mandates. The law creates personal liability for illegalor unauthorized acts, while making little effort to ensure that internet service providersor network service providers, as well as entities handling data, be responsible for its safedistribution or processing."

Digital Personal Data Protection Act, 2023 Applicability

The Digital Personal Data Protection Act of 2023[345] serves as a vital safeguard for individual privacy in the digital age. Its applicability is paramount in ensuring that personal data is handled responsibly and ethically across various sectors.

First and foremost, the act applies to all entities, both public and private, that collect, process, or store personal data in digital formats. This broad scope encompasses businesses, government agencies, and service providers alike. By encompassing such a wide range of entities, the act aims to create a comprehensive framework for protecting personal privacy in the digital realm.

Within this framework, the act establishes clear guidelines for the collection, processing, and storage of personal data.[346] It requires organizations to obtain explicit consent from individuals before collecting their data and to use that data only for specified purposes. This ensures that individuals have control over how their personal information is used and empowers them to make informed decisions about their privacy.

Moreover, the act imposes stringent security measures to safeguard personal data against unauthorized access, disclosure, or alteration. It requires organizations to implement robust data protection protocols and to notify individuals promptly in the event of a data breach. By holding organizations accountable for the security of personal data, the act reinforces individuals' trust in digital platforms and services.

Additionally, the act grants individuals certain rights regarding their personal data, such as the right to access, rectify, or delete their information. These rights empower individuals to exercise greater control over their digital footprint and to hold

[345] The Digital Personal Data Protection Act, 2023 (No. 22 of 2023), Gazette of India, August 11, 2023, https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf
[346] Ibid

organizations accountable for their data practices.

In essence, the Digital Personal Data Protection Act of 2023 plays a pivotal role in upholding personal privacy in the digital age. By establishing clear standards, rights, and responsibilities, it fosters a culture of transparency, accountability, and trust in the handling of personal data. Through its comprehensive approach, the act seeks to balance the legitimate interests of businesses and governments with the fundamental rights of individuals, thereby ensuring a fair and equitable digital ecosystem.

Personal Data Definition under the 2019 Bill

The definition of 'personal data' under the 2019 Bill has been significantly broadened to studied as “personal data implies data around or relating to a characteristicindividual who is straightforwardly or by implication identifiable, having respect to any characteristic, trait, property or any other include of the character of such normal individual, whether online or offline, or any combination of such highlights with any other data[347], and should incorporate deduction drawn from such data for the reason of profiling.”[348]

Under the 2018 Bill, personal data has awful been defined to cruel “data almostor relating to a natural person who is straightforwardly or in a roundabout wayidentifiable, having respect to any characteristic, trait, quality or any other highlight of the personality of such characteristic individual, or any combination of such highlights,or any combination of such highlights with any other information.[349] The extension of the definition of personal data is without a doubt a welcome degree because it broadensthe ambit of the 2019 Bill, reinforcing the privacy rights of information principals in return. Advance, the definition moreover covers any deduction drawn from personal data for the reason of profiling since such deduction ordinarily leads to roundabout distinguishing proof of a common person. This can be vital as certain substances utilizing advanced innovations carry on focusing on online promotion and utilize an individual's online exercises and design to customize their notices. In spite of the fact

[347] Section 3 (28) of The Personal Data Protection Bill, 2019.

[348] Section 3 (32) of The Personal Data Protection Bill, 2019 defines 'profiling' as "any form of processing of personal data that analyses or predicts aspects concerning the behaviour, attributes or interests of a dataprincipal."

[349] Section 3 (29) of The Personal Data Protection Bill, 2018.

that data accumulated from one's online exercises may not be competent of distinguishing a person exclusively", but when taken collectively or in combination with other characteristics, may result in distinguishing a person.

Amended Definition of Personal Data under Digital Personal Data Protection Act, 2023

In accordance with the Digital Personal Data Protection Act of 2023, **"personal data"** encompasses a broad spectrum of information relating to identified or identifiable individuals.

"Personal Data" is defined under section 2(t) of Digital Personal Data Act, 2023 as:

> ***(t) "personal data" means any data about an individual who is identifiable by or in relation to such data;***[350]

This definition includes but is not limited to fundamental identifiers like names, addresses, contact numbers, and official identification codes such as social security or passport numbers. Moreover, personal data extends to demographic particulars like age, gender, ethnicity, nationality, marital status, and linguistic preferences. Biometric data, comprising distinctive physical or behavioral characteristics like fingerprints, facial patterns, iris scans, and voiceprints, is also included. Financial particulars, such as bank account details, credit card information, income, and transaction records, fall within this category. Furthermore, sensitive health and medical information, genetic data, and details regarding healthcare services received are considered personal data, warranting heightened protection. Location data revealing an individual's whereabouts, like GPS coordinates or IP addresses, is encompassed as well. Even online identifiers, like usernames, social media profiles, device identifiers, and cookies, are recognized as personal data. This comprehensive definition underpins the Act's objective of safeguarding individuals' privacy in an increasingly digital landscape, reflecting the evolving nature of data and the imperative to protect it.

Process of Personal Data

The 2018 Bill expressed that personal data may be handled in case such handlingis vital

[350] Section 2 (t) of Digital Personal Data Protection Act, 2023.

for any work of the Parliament or any state council. The 2019 Bill has erased this arrangement and constrained the preparing of personal data, without assent of information vital, for arrangement of any benefit or advantage to the information vital from the State or for the issuance of any certification, permit or allow for any activity or action of the information central by the State, with regard to the capacities of the state authorized by law.[351] "The 2018 Bill expressed that individual information can be prepared, without assent, for certain sensible purposes as may be indicated by the Specialist. The Specialist may indicate the sensible purposes which incorporates the anticipation and location of any illegal movement counting extortion, shriek blowing, mergers and acquisitions, organize and data security, credit scoring, recuperation of obligation, preparing of freely accessible personal data.

The 2019 Bill has broadened the ambit of 'reasonable purposes' by including 'operation of look engines' to the list, which subject to certain conditions may be informed as a sensible reason. In this manner, personal data may be prepared without the assent of the information principal for the reason of operations of look engines. Although the degree and scope of passable handling of personal data under this head will be managed by the directions, this will, in all probability, be seen as a welcome move by companies working look motors who would have been something else excessive burdened by compliance prerequisites to get assent of information principals– that may prevent the effectiveness of their benefit".

The Digital Personal Data Protection Act of 2023 delineates a clear framework for the processing of personal data, ensuring that it is handled with due diligence and respect for individual privacy rights. The process of personal data, as outlined in the Act, encompasses a range of activities involved in the collection, storage, use, and sharing of personal information.

Firstly, organizations must transparently inform individuals about the purposes for which their personal data is being collected and processed. This entails obtaining explicit consent from data subjects before initiating any data processing activities, except in cases where processing is justified by law or necessary for the performance of a contract.

Once consent is obtained, organizations are responsible for processing personal data in accordance with the principles of legality, fairness, and transparency. This includes

[351] Section 12(a) (i) and (ii) of The Personal Data Protection Bill, 2019.

ensuring that data processing activities are carried out for legitimate purposes, without unlawfully infringing upon individuals' rights or interests.

Furthermore, the Act imposes obligations on organizations to implement appropriate technical and organizational measures to safeguard personal data against unauthorized access, disclosure, alteration, or destruction. This may involve encryption, pseudonymization, access controls, and regular security assessments to mitigate risks to data security and integrity.

Additionally, organizations are required to uphold individuals' rights with respect to their personal data, including the right to access, rectify, erase, or restrict the processing of their information. Data subjects must also be informed of their rights and provided with mechanisms to exercise them effectively.

Moreover, the Act prohibits the transfer of personal data to third parties or foreign jurisdictions that do not provide an adequate level of data protection, unless certain safeguards are in place to ensure the continued protection of individuals' rights.

Overall, the process of personal data under the Digital Personal Data Protection Act of 2023 is governed by principles of accountability, transparency, and respect for individuals' privacy rights. By establishing clear guidelines and obligations for data controllers and processors, the Act seeks to foster trust and confidence in the handling of personal data in the digital age.

Additional Right of Data Principal under The Digital Personal Data Protection Act of 2023

The Digital Personal Data Protection Act of 2023 introduces several additional rights for data principals,[352] aiming to empower individuals with greater control over their personal data and enhance their privacy protections in the digital realm. Among these rights, perhaps one of the most significant is the right to data portability.

Data portability grants individuals the ability to obtain and reuse their personal data for their own purposes across different services or platforms. This means that individuals can request their data from one organization and transfer it to another organization seamlessly, without hindrance or obstruction. For example, a social media user may request a copy of their profile information, posts, and photos from one social media platform and transfer it to a competing platform of their choice.

[352] Section 2 (j) of Digital Personal Data Protection Act, 2023.

By enabling data portability, the Act promotes competition, innovation, and consumer choice in the digital marketplace. It empowers individuals to switch between service providers more easily, fostering a dynamic and competitive environment where organizations are incentivized to offer better services and data protection practices to retain customers.

Moreover, data portability enhances individuals' autonomy and control over their personal information, aligning with principles of data sovereignty and self-determination. It ensures that individuals are not locked into proprietary ecosystems or beholden to a single organization for access to their own data, thereby promoting a more equitable and user-centric approach to data management.

However, it's essential to note that the right to data portability is subject to certain limitations and conditions under the Act. Organizations may impose reasonable restrictions on the exercise of this right to protect the rights and freedoms of other individuals, safeguard confidential information, or ensure compliance with legal obligations.

Overall, the inclusion of data portability as an additional right under the Digital Personal Data Protection Act of 2023 represents a significant step forward in strengthening individuals' privacy rights and promoting a more transparent, accountable, and user-centric approach to data governance in the digital age.

The Right to Data Elimination

Under the Digital Personal Data Protection Act of 2023, the right to data elimination is enshrined as a fundamental protection for individuals' privacy rights. This right empowers data principals to request the deletion or removal of their personal data from the databases or systems of data controllers under certain circumstances.

Section 5[353] of the Act outlines the specific provisions regarding the right to data elimination. According to this section, data principals have the right to request the deletion of their personal data when it is no longer necessary for the purposes for which it was collected or processed, when consent for processing is withdrawn, or when the data processing is deemed unlawful.

Furthermore, Section 5[354] also stipulates that data controllers must comply with

[353] Obligations of Data fiduciary
[354] Ibid

requests for data elimination within a reasonable timeframe. Failure to comply with these obligations may result in penalties or sanctions imposed by the relevant data protection authorities.

The right to data elimination is crucial for empowering individuals to maintain control over their personal information and to ensure that their data is not retained indefinitely without a legitimate purpose. By providing individuals with the ability to request the deletion of their data, the Act promotes accountability, transparency, and respect for individuals' privacy rights within the digital ecosystem.

In summary, the Digital Personal Data Protection Act of 2023 recognizes the right to data elimination as an essential component of comprehensive data protection legislation. By establishing clear provisions and obligations regarding the deletion of personal data, the Act aims to uphold individuals' rights to privacy and data sovereignty in the digital age.

Privacy by Design Policy

The Digital Personal Data Protection Act of 2023 emphasizes the principle of Privacy by Design, which entails integrating privacy considerations into the design and development of systems, processes, and products from the outset. This proactive approach to privacy aims to minimize the risk of privacy breaches and enhance data protection throughout the lifecycle of personal data.

Section 8[355] of the Act specifically addresses Privacy by Design, requiring organizations to implement privacy-enhancing measures at every stage of data processing. According to this section, data controllers and processors must incorporate privacy features into their systems and operations, ensuring that personal data is protected by default.

Furthermore, Section 8[356] mandates that organizations conduct privacy impact assessments (PIAs) to identify and mitigate potential privacy risks associated with their data processing activities. These assessments help organizations evaluate the privacy implications of their projects, products, or services and implement appropriate safeguards to protect individuals' personal data.

Moreover, Section 8[357] underscores the importance of data minimization and purpose

[355] General obligations of Data Fiduciary
[356] Ibid
[357] Ibid

limitation, requiring organizations to collect only the personal data that is necessary for the specified purposes and to retain it only for as long as necessary to fulfill those purposes.

In addition to these requirements, Section 8[358] encourages organizations to adopt privacy-enhancing technologies and practices, such as encryption, anonymization, and pseudonymization, to further protect personal data from unauthorized access or disclosure.

By embedding Privacy by Design principles into their policies and practices, organizations can foster a culture of privacy and data protection, instilling trust and confidence in their customers and stakeholders. This proactive approach not only helps organizations comply with the requirements of the Digital Personal Data Protection Act but also enables them to adapt to evolving privacy regulations and consumer expectations in an increasingly data-driven world.

New Recognized Categories of Data Fiduciaries under The Digital Personal Data Protection Act of 2023

The Digital Personal Data Protection Act of 2023 introduces innovative categories of data fiduciaries, reflecting the evolving landscape of data processing and privacy concerns. Section 10[359] of the Act delineates the criteria for identifying these fiduciaries and recognizes several new categories.

Firstly, the Act designates "Social Media Platforms" as a distinct category of data fiduciaries. These platforms play a central role in collecting, processing, and disseminating personal data, warranting specific regulations to address privacy risks. As data fiduciaries, social media platforms are obligated to adhere to stringent data protection standards, ensuring transparency, consent, and security in their data processing practices.

Secondly, the Act identifies "Internet of Things (IoT) Device Manufacturers" as another category of data fiduciaries. With the proliferation of connected devices, such as smart home appliances and wearable technology, IoT device manufacturers are entrusted with vast amounts of personal data. Recognizing them as data fiduciaries underscores the importance of safeguarding user privacy and implementing privacy-by-design

[358] Ibid

[359] Additional obligations of Significant Data Fiduciary

principles in IoT product development.

Additionally, the Act acknowledges "Data Analytics Firms" as a distinct category of data fiduciaries. These firms specialize in analyzing large datasets to extract valuable insights, often involving the processing of personal data. By recognizing data analytics firms as data fiduciaries, the Act aims to ensure responsible data handling practices and transparency in data analytics processes.

Furthermore, the Act may recognize additional categories of data fiduciaries based on emerging technologies or data processing activities that pose significant privacy risks. This forward-thinking approach enables the legislation to adapt to evolving data practices and technological advancements, ensuring comprehensive protection for individuals' personal data.

In essence, the recognition of these new categories of data fiduciaries under the Digital Personal Data Protection Act reflects a proactive stance towards addressing privacy challenges in the digital age. By imposing specific obligations on these entities, the Act aims to foster a culture of privacy, accountability, and trust in data processing activities, ultimately enhancing individuals' control over their personal data.

Restriction on Cross-border Transfer of Personal Data

The Digital Personal Data Protection Act of 2023 imposes strict restrictions on the cross-border transfer of personal data to ensure the continued protection of individuals' privacy rights even when their data moves beyond national borders. Section 16[360] of the Act outlines these restrictions and establishes the conditions under which such transfers are permissible.

According to the Act, data controllers are prohibited from transferring personal data to jurisdictions that do not provide an adequate level of data protection, unless certain safeguards are in place to protect the rights and freedoms of data subjects. This requirement is in line with international standards and best practices for data protection, which emphasize the importance of ensuring that personal data is subject to comparable levels of protection regardless of where it is processed or stored.

Furthermore, Section 16[361] specifies that data controllers must conduct a comprehensive assessment of the data protection laws and practices in the recipient

[360] Processing of personal data outside India.
[361] Ibid

jurisdiction to determine whether it provides an adequate level of protection for the personal data being transferred. If the recipient jurisdiction does not meet the required standards, data controllers must implement additional safeguards, such as contractual clauses, binding corporate rules, or obtaining explicit consent from data subjects, to ensure the continued protection of personal data.

Moreover, the Act empowers the relevant data protection authority to oversee and regulate cross-border data transfers, including conducting audits, investigations, and enforcement actions to ensure compliance with the Act's provisions. Data controllers found to be in violation of the Act's restrictions on cross-border data transfers may be subject to penalties, sanctions, or other enforcement measures as prescribed by the Act.

Overall, the Digital Personal Data Protection Act of 2023 establishes robust safeguards to regulate the cross-border transfer of personal data and protect individuals' privacy rights in an increasingly globalized digital economy. By imposing stringent requirements on data controllers and providing oversight mechanisms to enforce compliance, the Act aims to ensure that personal data is handled responsibly and ethically across borders, maintaining trust and confidence in the digital ecosystem.

Exemption for Government agencies

The Digital Personal Data Protection Act of 2023 outlines exemptions for government agencies under certain circumstances, recognizing the unique roles and responsibilities they hold in the processing of personal data for public interest purposes. Section 17[362] of the Act delineates these exemptions and provides clarity on the conditions under which government agencies may be exempt from certain provisions of the Act.

According to the Act, government agencies may be exempt from certain requirements of the Act if compliance would impede the performance of their functions or if it is necessary for reasons of national security, public order, or other compelling public interests. This exemption acknowledges that government agencies often process personal data for essential public services and functions, such as law enforcement, national defense, or public health, where strict compliance with certain provisions of the Act may be impractical or infeasible.

However, it's important to note that the exemption for government agencies is not

[362] Exemptions

absolute. Section 17[363] specifies that any exemption granted to government agencies must be necessary and proportionate to the public interest pursued, and must not unduly infringe upon individuals' privacy rights. Additionally, government agencies are still required to comply with the core principles of data protection, such as transparency, fairness, and security, to the extent feasible given the nature of their functions and responsibilities.

Furthermore, the Act stipulates that government agencies must designate a data protection officer responsible for overseeing compliance with data protection requirements and handling inquiries or complaints related to the processing of personal data by the agency. This requirement ensures accountability and transparency in the processing of personal data by government agencies, even in cases where exemptions may apply.

In summary, the Digital Personal Data Protection Act of 2023 strikes a balance between safeguarding individuals' privacy rights and recognizing the legitimate interests of government agencies in processing personal data for public interest purposes. By providing exemptions under certain conditions and imposing accountability measures, the Act aims to ensure responsible and lawful data processing practices by government agencies while upholding privacy protections for individuals.

[363] Ibid

Chapter-9

Judiciary and Right to Privacy

Today, India does not have comprehensive laws on the protection of personal data that guarantees the right of people to privacy and to address personal data protection. The constitution itself does not explicitly guarantee the right to privacy as a fundamental right. The place of the right if it exists must therefore be located within the structure of the constitution as came out by judicial decisions. The Indian judicial system, as referred to in Articles 19(1) (a) and 21 of the Indian Constitution, has regarded the rights to privacy as a basic right. The Indian Judiciary has, in its case by case since the 1960s, articulated the right to privacy.

Although the Indian judicial authority has never defined privacy in any way, in some situations it interprets the right, including a person's family, marriage, maternity, child-care, and education, to be the impacts of a person's life.

"There is no guaranteed right to privacy in the Indian Constitution and it could not be found in any other statute. However, interests similar to that are protected both under statutory law, that is, under the Indian Penal Code or the Indian Evidence Act, and under the Constitution of India."

"These rights have been given different nomenclaturein the form of privileged communication, withholding of documents, domestic affairs, matrimonial rights etc. The Supreme Court has evolved through decisions various rights,interests in all cases similar to privacy, for example right of free enjoyment, right to sleep, right to human dignity, right to have access to justice, right to speedy trial, emanating from the concept of personal liberty in Article 21 of the Constitution. But it does not cover, at one place, all the interests of privacy which need protection."

Right to Privacy in Pre- Independence

"Indian judicial history indicates that privacy, as a right was recognized as a part of custom from ancient times and received statutory recognition in Section 18

of the Easements Act, 1882. To reiterate, the first case, which was decided by the Sadar DiwaniAdalat in 1855 deals with the question of privacy right." Reference to this case was madeby Chief Justice Edge in *Gokal Prasad* v. *Radho.*[364]

Searches and Seizures in Right to Privacy

"The right to privacy vis-a-vis police method of crime control is, therefore, subject to police method of surveillance and the crime control to be effective the provisoin the decision of the Supreme Court in Govinda's case should also go. Besides, the Supreme Court in *M. P. Sharma* v. *Satish Chandra*,[365] has frowned upon elevating the right to privacy to the status of fundamental right. The instant case was the first case before the Supreme Court wherein the court had the opportunity of considering the constitutional status of the right to privacy in context of state power of search and seizure. The police on information that Dalmia Group of Companies were engaged in fraudulent practices carried out a search and seized voluminous documents under of validly issued search warrant. The petitioner challenged the very search warrant under Article 32 of the Constitution contending that the search warrants were violated of Articles 20(3) and 19(l)(g) of the Constitution."

The search warrant was issued under Section 96 of the Criminal Procedure Code and the court upheld the constitutional validity of this section by observing that:

"the power of search and seizure is in any system of jurisprudence an overriding power of the State for the protectionof social security and that power is necessarily regulated by law".

Justice Jagannadha das speaking for the Court observed:

"When the Constitution makers have thought fit not to subject such regulation to constitutional limitations by recognition of a fundamental right to privacy, analogous to the American Fourteenth Amendment, we have no justification to import it intoa

[364] ILR 10 All. 358 (1888)
[365] AIR 1954 SC 300

totally different fundamental right by some process of strainedconstruction".[366]

"The above observation of Justice Jagunnadhadas can be considered valid in sofar some different aspects of this particular case were concerned, but since there is an increasing tendency to life judgments out of their relevant context for citation in other cases having entirely different merits on the part of litigants, there is possibility that such generalization may harm the theme of privacy as a fundamental right". With regard to the concept of privacy, therefore, "the researcher can draw the following conclusions;

a. The right to privacy can only be read directly but impliedly in Article 21of the Constitution, and indirectly in Article 19, and
b. whether they be the safeguards under Section 96 of the Code of Criminal Procedure or under Article 20(3) of the Constitution, they suffer from inherent defect that they do not grant privacy so far as they also remain limited and confined to criminal cases.

These safeguards do not extend to parties and witnesses in civil proceedings or proceedings other than criminal. They do not have any utility in other proceedings and it is only Article 21 which can ensure right to privacy".

In *Board of Revenue, Madras* v. *R. S. Jhavar,*[367] "the Supreme Court held that the power of search and seizure can be exercised by an administrative authority only when it is conferred on it by a statute. The stipulations made by the statutes in questionregulating the power of search and seizure must be observed by the authority concerned,otherwise search and seizure will be declared illegal and nothing recovered at such a search can be made use of an evidence against the individual concerned".

In *Pooram Mai* v. *Director Inspection,*[368] also "the Supreme Court itself frowned upon such construction holding that neither by invoking the spirit of our Constitution nor by a strained construction of any of the fundamental rights can we spell out the exclusion of evidence obtained by an illegal search.[369] The Supreme Court thus restricted the right to privacy vis-a-vis search and seizure.

[366] Ibid
[367] AIR 1968 SC 59.
[368] AIR 1974 SC 348.
[369] Ibid

Further, in the case of *Deena* v. *Union of India*,[370] the Supreme Court held that as judges they ought not to assume that they are endowed with a divine insight into the needs of society. On the contrary they should heed the warning that history simply proves that judiciary is prone to misconceive the public good by confounding private notions with constitutional requirements".[371]

In People's *Union for Civil Liberties* v. *Union of India*[372], "the Supreme Court held that wiretapping is a serious invasion of an individual's privacy. The court observedthat telephonic conversation is a part of a man's private life. And certainly, right to privacy includes telephonic conversation in the privacy of one's home or office".

In *District Registrar and Collector* v. *Canara Bank*,[373] "the court struck down Section 73 of the Indian Stamp Act, 1899 as amended by the Andhra Pradesh Act (17 0f 1986) as permitting an overbroad invasion of private premises or the homes of persons in possession of documents in a power of search as seizure without guidelines as to who and when and for what reasons can be empowered to search and seize, and impound the documents. The Court held that the right to privacy dealt with persons andnot places. The court, however, held that no right to privacy could be available for any matter which is part of public records including court records".

In *Ram Jethmalani* v. *Union of India*,[374] "the Supreme Court held that revelation of an individual's bank accounts without any prima facie ground of wrongdoing is violation of his right to privacy. The Supreme Court observed:

Right to privacy "is an integral part of right to life, this is a cherished constitutional value, and it is important that human beings be allowed domains of freedom that are free of public scrutiny unless they act in an unlawful manner."

---

[370] AIR 1983 SC 1155.
[371] Ibid
[372] AIR 1997 SC 568.
[373] AIR 2005 SC 186.
[374] (2011) 8 SCC 1.

In *Selvi* v. *State of Karnataka*[375], "the Supreme Court held that compulsory administration of any of the techniques, like narco analysis, polygraph examination andbrain Electrical Activation Profile(BEAP) test, is an unjustified intrusion into the mentalprivacy of an individual. It was also recognized that forcible intrusion into a person's mental processes is also an affront to human dignity and liberty, often with grave and long-lasting consequences".

In *Re: Ramlila Maidan Incident Dt. 4/5.06.2011* v. *Home Secretary, Union of India and others*,[376] "decided on 23 February, 2012, the Supreme Court noted that evenif an assembly was illegal, the action of police under Section 144 of Code of Criminal Procedure (Cr PC) without being preceded by an announcement to the sleeping individuals was not reasonable. The court observed that 'Sleep' is a basic requirement for the survival of every human life. Furthermore, to disturb someone's sleep is a violation of his or her human right as it amounts to torture. Therefore, the court declaredthat right of privacy of sleeping individuals was immodestly and brutally outraged by the State police action".

Natural Modesty and Morality in Right to Privacy

"In order to protect the privacy of women intruding upon the privacy of woman is made as an offence and is punishable under Section 509 of the Indian Penal Code. The criminal action is envisaged by Section 509 of the Indian Penal Code for violatingthe privacy of women. Where the offence charged consists of the accused's intrusion upon the privacy of a woman, it must show that the intrusion was made with intent to insult the modesty of any woman.[377] The accused, a stranger, though a neighbor, entered at night into the room where four women were sleeping and on an alarm being given and attempt made to capture him, the accused escaped. It was held that the intrusion upon the privacy was sufficient to bring it within the scope of this section".[378]

In *Neera Mathur* v. *Life Insurance Corporation of India*,[379] "the petitioner was

[375] 2010(4) SCALE 690.
[376] (2012) 5 SCC 1.
[377] Phaiz Mohammed 5 Bom.LR 502, Hopper 1192 reported in Law of Crimes and Criminology, R. P. Kathuria, Vol. 3, pp. 4035 (2000).
[378] 1895 ILR 22 Cal. 994.
[379] AIR 1992 SC 392,

appointed in respondent's service and was on probation. She was pregnant at the time and took maternity leave for three months. She was discharged subsequently from service. It was alleged that she gave false declaration regarding the last menstruation period and thereby suppressed the fact of pregnancy". The Supreme Court observed:

"The real mischief though unintended is about the nature of thedeclaration required from a lady candidate. The particulars to be furnished under columns (iii) to (viii) in the declaration are indeed embarrassing if not humiliating. The modesty and self- respect may perhaps preclude the disclosure of such personal problems like whether her menstrual period is regular or painless, the number of conceptions taken place; how many havegone full terms etc. The Corporation would do well to delete suchcolumns in the declaration."

Hence, "any quarry with respect to above nature would adversely affect the modesty and self-respect and would attract the right to privacy of a woman.

In *Nihal Chand* v. *Bhagwan Dei*,[380] the Allahabad High Court while emphasizing the importance of right to privacy, observed that the right to privacy is based on naturalmodesty and human morality. It is not confined to any class, creed, color and is very sacred".

Freedom of Press and Right to Privacy

"Freedom of Press has been acclaimed as the cornerstone of modem democratic State. It is often described as fourth estate *Himachal Pradesh* v. *Umed Ram*;[381] The Pressenjoys a prestigious position in democratic countries where constitution's guarantee freedom or press. The freedom, like all other liberties, cannot be absolute and is subjectto restrictions in public interest. Privacy of individual is a right to be protected even from the gaze of press. Invasion of privacy may arise when information about private affairs of a person is published by newspaper *P. Rathinam* v. *Union of India*;[382] James Michael elucidates the difference between privacy and defamation thus:

Some complaints about invasion of privacy by the press are about the techniques

[380] AIR 1935 AU 1002.
[381] AIR 1986 SC 847
[382] AIR 1984 SC 1844.

used in attempting to get information, others are about the publication of personal information, and many are about both. Concern about invasions of privacy by the pressare often mixed with concern about defamation, and it is perhaps worthwhile to recall the difference. Invasion of privacy, in the sense of informational privacy, by the press is, in Prosser's terms, the disclosure of embarrassing private facts. Defamation is the publication of damaging information which is false. Without going into details about the burden of proving truth or not, privacy is about the true information, defamationabout false".[383]

"Is there a right to publish true or unwelcome or damaging information about the people? Geoffrey Marshall states:[384] 'anybody asked to answer this question in a particular case would want to know and weigh four considerations assuming theinformation to be true. They are,

a. was the information acquired properly or innocently, or by wrongful means;
b. was there any consent to disclosure or would anybe implied;
c. was the activity described exposed itself innocent or disreputable; and
d. was there any actual damage caused to just annoyance

These questions must arise in cases of unwarranted disclosure of information. It is obvious that they necessitate themaking of choice between different values. The law cannot, by itself, decide them finallyby legal principles alone. It is to be borne in mind that 'free speech is sabotaged from within by fouling the fountains of information.'[385] When the court or legislatures expandthe protection given to privacy, they may limit the media's freedom to report and the public's right to know".[386]

"To keep the Press as a strong medium that can safeguard public interest it must observe self-censorship with a set of norms based on sound principles that due regard to both freedom of expression and right to privacy. In this regard,

---

[383] James Michael, "Privacy" in Individual Rights and Law In Britain in Christopher Mc Crudden andGerals Chambers (edition),

[384] Bakshi, P. M. Defamation and Privacy in Law of Defamation: Some Aspects 20 (1986) quoted fromGeoffrey Marshall, The Right to Privacy - A Sceptical View, MC Gill L.J.,

[385] Iyer; V. R. Krishna, The Right to Know is Fundamental in Salvaging Democracy 119 (1990).

[386] William A. Hachten, The Supreme Court on Freedom of the Press: Decisions and Dissents 166 (1970).

Press Council can play an effective role by giving proper direction to the print media. Professor Rajeev Dhavan opines that the court is giving recognition to the institutional right of press to act as a watchdog on the effective governance of administration.[387] According to Soli J.Sorabjee, the major premise of the ruling in R. Rajagopal is that uninhabited discussionof public affairs is essential in a democracy and the possibility of error is inevitable. If media were to be held liable for every error inaccuracy, absent malice or reckless disregard for truth, the consequent 'chilling effect' would generate self-censorship in media about matters of public concern.[388] In case the publication has no relation to official conduct and is defamatory, the public official has the same remedy available to an ordinary individual".

Telephone-Tapping and Right to Privacy

"Telephonic-tapping is a serious invasion of the right to privacy. One can tap the telephone lines and listen to others talking. Some persons may use it for their personal pleasure, some for commercial gains and we find the Government using it on the pretextof surveillance. In all these instances, right to privacy was the victim. There is however,no express guarantee against the telephone-tapping under the Constitution of India".

In "*Yusuf Ali Ismail Nagree* v. *State of Maharashtra*,[389] the court was faced with the question whether tapping of the appellant's conversation without his knowledge offended his right under Article 21. In this case, the police inspector tapped the conversation between Nagree and Sheikh, a municipal clerk whom Nagree wanted to bribe. Nagree had no knowledge of this. Nagree challenged the admissibility of such evidence. The court evolved two directions for guidance in admitting such evidence. First, the court will find out whether it is genuine and free from tampering or mutilations.Secondly, the court may also secure scrupulous conduct and behavior on behalf of thepolice. The reason is that the police officer is more likely to behave properly if improperly obtained evidence is to be viewed with care and caution by the judge. In every case the position of the accused,

[387] Rakesh Bhatnagar, An Extraordinary Bold Verdict, Times of India, 16 (Oct 15, 1995).

[388] Soli J. Sorabjee, Privacy and Defamation: SC Defines Parameters, Indian Express 8 (November 12,1994)

[389] AIR 1973 SC 157,

the nature of investigation and the gravity of theoffence must be judged in the light of material facts and the surrounding circumstances."

"The court further rejected the appellant's arguments that it violated procedures established by law and the appellant was incriminated. Conversation was voluntary andwithout any compulsion. The attaching of tape-recording machine was known to the appellant, that fact does not render the evidence inadmissible. The tape was only a mechanical contrivance to play the role of eavesdropper. The court also rejected the appellant's argument that his right to privacy was violated. It said Article 21 contemplates procedure established by law with regard to deprivation of life or personalliberty. The telephonic conversation of an innocent citizen would be protected by courtsagainst wrongful or highhanded interference by tapping the conversation. The protectionis not for a guilty citizen against the efforts of police to vindicate the law and prevent corruption in public servants. It must not be understood that the courts would tolerate safeguards for the protection of the citizen to be imperiled by permitting the police to proceed by unlawful or irregular methods. In the present case, no unlawful or irregular method was adopted in obtaining the tape-recording conversation".

In "*Rama Reddy* v. *V. V. Giri*,[390] the Court held that the tape-recording conversation is admissible provided first the conversation is relevant to the matter in issue, secondly, there is identification of voice, thirdly, the accuracy of the tape-recordedconversation is proved by eliminating the possibility of erasing the tape recorded. Further, in *Megraj Patodia* v. *R. K. Birla*,[391] the Supreme Court clearly stated that a document which was procured by improper or even illegal means could not bar its admissibility provided its relevance and genuineness were proved."

The challenge to "telephone-tapping under Article 21 was considered in *R. M. Malkani* v. *State of Maharashtra*.[392] in this case, the telephonic conversation between two parties was tape-recorded by the police with the consent of one of the parties. The Supreme Court observed that the conversation could be used in evidence as it was voluntary and there was no duress or compulsion to extract

[390] AIR 1968 SC 147
[391] (1971) IS.C.R.399.
[392] AIR 1971 SC 1295.

the same. The fact that the tape-recording instrument was attached without appellant's knowledge does not make the conversation inadmissible against him. The Supreme Court further observed that it would not tolerate safeguards for the protection of citizen to be imperiled by permittingthe police to proceed by unlawful or irregular methods. At the same time the court held that even stolen evidence was admissible if it was not tainted by an inadmissible confessof guilt".

In "*Peoples Union for Civil Liberties* v. *Union of India*,[393] the Supreme Court examined in detail the challenge to the right to privacy by way of telephone-tapping. The court looked into the constitutional validity of Section 5(2) of the Indian TelegraphAct, 1885, by virtue of which the government has tapped some telephonic conversations.After holding that privacy is an essential ingredient of personal liberty, Kuldeep Singh, J. came to the conclusion that telephone tapping is a serious invasion of an individual'sprivacy. He observed that with the growth of highly sophisticated communication technology, the right to hold telephone conversation in the privacy of one's home or office without interference is increasingly susceptible to abuse. It was held that telephone-tapping, a form of 'technological eavesdropping' infringed the right to privacy. Finding that the Government had failed to lay down a proper procedure under Section 7(2) (b) of the Act to ensure procedural safeguards against the misuse of the power under Section 5(2), the court prescribed stringent measures to protect the individual's privacy to the extent possible".

"Taking cue from the earlier decisions, in this public interest litigation, the Supreme Court had no hesitation in holding that right to privacy is part of the right to 'life and personal liberty' enshrined in Article 21 of the Constitution and the said right cannot be curtailed, except according to procedure established by law."[394]

"In this case, the constitutional validity of tapping of politician phones by the Central Bureau of Investigation was challenged as it amounts to violation of right to privacy. It was contended that right to privacy is a fundamental right guaranteed under Article 19(1) and Article 21 of the Constitution of India. The

[393] AIR 1997 SC 568
[394] Ibid

Supreme Court after reviewing the earlier cases in this field held that 'we have, therefore, no hesitation in holding that rightto privacy is a part of the right to life and personal liberty enshrined under Article 21 ofthe Constitution. Once the facts in a given case constitute a right to privacy Article 21 is attracted. The said right cannot be curtailed 'except according to procedure established by law.' It may thus be summed up that in India constitutional provisions oftelephonic interception lack the clarity and depth of its American counterpart. This canbe attributed to three main reasons, viz. firstly, the courts have never defined the parameters of right to privacy with regard to electronic interception in the way Americancourts have done in the Katz case.[395] Telephonic conversation has been taken out from the overall context of electronic snooping and dealt with. But even there the exact rightto privacy vis-a-vis wiretap has been dealt in a superficial manner. Secondly, the telephonic interception has been treated as infringement of Article 19(1)(a). Thisprevents wiretap for any other purpose than those enumerated in Article 19(2) causing hindrance to law enforcement. Lastly, in India wiretap does not require a judicial warrant, nor is there any exclusionary rule of evidence. This leaves the aggrieved personwithout a remedy in case a violation of this right occurs. The law of wiretap in India is therefore, satisfactory neither from the point of view of the law enforcement nor the accused. One can only hope that the legislature and the courts take notice of this".

Restitution of Conjugal Rights and Right to Privacy

"The conjugal right that is, the right of the husband or the wife to the society ofother is not the creature of statute. But it is inherent in the very institution of marriage itself. The Law Commission of India in its 71st Report stated that the essence of marriageis a sharing of common life, a sharing of all the happiness that life has to offer and all the miseries that has to be faced in life, an experience of the joy that comes from enjoying the common things of the matter and of the spirit and fi-om showering love and affection of one offspring. The remedy of restitution of conjugal rights and its origin in the ecclesiastical law of England. But now it has been abolished in England bythe Matrimonial Proceeding

[395] Katz v. United States, 389 U.S. 347 (1967)

Act, 1970. In India, it was applied as a part of justice, equityand good conscience. However, Hindu Marriage Act, 1955, enacted it as statutory remedy".

"Fundamental rights jurisprudence witnessed another development in the first half of 1980s wherein constitutionality of Section 9 of the Hindu Marriage Act, 1955 providing for restitution of conjugal rights was challenged on the ground of violation ofArticle 21 in *T. Sareetha* v. *T. Venkata Subbaiah*.[396] The court declared Section 9 as ultra vires and violated of Articles 14 and 21 of the Constitution. Chaudhary, J. while examining restitution of conjugal rights in relation to right to personal liberty opined: A decree of restitution of conjugal rights constitutes the grossest form ofviolation of an individual's right to privacy. It denies women her choice whether, whenand how, her body is to become the vehicle for the procreation of another human being."

"Justice Chaudhary has no hesitation in characterizing the remedy of restitution of conjugal rights as a savage and barbarous remedy, violating the right to privacy and human dignity guaranteed by Article 21 of our Constitution. The court was prepared toaccord zones of privacy to each spouse even in the marital relationship". It was observed:

". . . a court decree enforcing restitution of conjugal right constitutes the starkest form of government invasion of personalidentity and individual's zone of intimate decisions. The victim isstripped of its control over the various parts of its body subjectedto the humiliating sexual molestation accompanied by a forcibleloss of the precious right to decide when if at all her body shouldbe allowed to be used to give birth to another human being. Clearly the victim loses its autonomy of control over intimacies of personal identity. Above all, the decree for restitution of conjugal rights takes the unwilling victims body of soulless and a joyless vehicle for bringing into existence another human being. In other words, pregnancy would be foisted on her by theState and against her will. There can therefore be little doubt that such a law violates the right to privacy and human dignity guaranteed by and contained in Article 21 of ourConstitution".[397]

The issue again cropped up "in *Harvinder Kaur* v. *Harminder Singh*.[398] Justice

[396] AIR 1983 AP 356.
[397] Ibid
[398] AIR 1984 Delhi 66.

Avadh Bihari Rohtagi of Delhi High Court has expressed a contrary view and upheld the validity of Section 9 of the Hindu Marriage Act. The court opined that though sex constitutes an important element in marriage but it does not constitute the sole object. Court opposed the introduction of constitutional principles in the privacy of a home. The court observed that in the privacy of a home Articles 14 and 21 have no place whatsoever, matrimonial relations are rather based on love, affection, care and like considerations".

"The Supreme Court finally set the controversy at rest in *Saroj Rani* v. *Sudarshan Kumar*[399] by approving the judgment of Delhi High Court in Harvinder Kaur's case. Supreme Court ruled that Section 9 serves social purpose as an aid to the preservation of marriage and therefore, satisfies Articles 14 and 21".

"In the present era AIDS has posed a new problem before courts regarding conjugal rights, right to privacy and right to information. The much appreciative step towards the protection of right to privacy of HIV infected persons is the direction of thecourt to suppress the identity of the AIDS patients in proceedings before the court became after disclosure of name, they suffer from several embarrassments including badpublicity and consequential discriminations in every walk of life. The appeal for suppression of identity before court was made in the case of *MX of Bombay Indian Inhabitant* v. *M/S ZY*.[400] In this case, the Division Bench passed an order permitting the petitioner to prosecute by suppressing the identity and therefore, to be named as 'Mr. MX' and also directed the respondent corporation to be named as 'ZY'. The learned counsels for the respondent addressed the court on the aspect of requirement of nondisclosure of identity of the petitioner in such matters and submitted that in view ofthe stigma which is attached to HIV infection, the persons infected with HIV may be reluctant to approach the court of law with fear that the disclosure of his HIV status mayexpose him to social ostracization and also discrimination in every walk of life. Hence,the apex court has categorically observed and permitted the suppression of density of the medically acquired HIV or AIDS cases. This decision protected privacy from the society. Another dimension or

[399] AIR 1984 S 1526
[400] AIR 1997 Bom 406.

right to privacy i.e. right to privacy of AIDS infected people has received judicial attention during the recent times. The question here arises is whether AIDS infected people have a right to privacy i.e. whether they have right thattheir HIV should be kept secret. The question has acquired immense importance in the present time. It will not be an exaggeration to say that the whole community is sitting on AIDS bomb ready to explode anytime.[401] In view of this, it is pertinent to examine the right to privacy of AIDS infected people".

In case [402] "the Supreme Court was seized on an issue concerning an AIDS patient and his right to privacy and confidentiality regarding his medical condition, and right of the lady to whom he was engaged to lead a healthy life.In this case, a person was found to be HIV positive and the information was disseminated by the doctor to his prospective wife. The person preferred a suit against the doctor for breach of right to privacy and damages as well".

"Doctor-patient relationship though basically commercial is professionally a matter of confidence and therefore, doctors are normally and ethically bound to maintain confidentiality. In such a situation public disclosure of even true private facts may amount to an invasion of the right to privacy which may sometimes lead to clash of one person's right to be let alone which another person's right to be informed."

"Disclosure of even true private facts has a tendency to disturb a person's tranquility. It may generate many complexes in him and may even lead to psychological problems. He may, thereafter, have a disturbed life all through. In the force of these potentialities the right of privacy is an essential component of right envisaged by the Article 21. Theright, however, is not absolute and may be lawfully restricted for the prevention of crime, disorder, or protection of health or morals or protection of rights and freedom ofothers. As such, when the patient was found to be HIV positive, its disclosure by the doctor would be violated of either the rule of confidentiality or the patient's right to privacy. However, there is another face of the coin also. Its disclosure would have saved the lady with whom the patient was likely to be married otherwise she too

[401] Sureder Kumar Singh, Human Rights of AIDS Infected People vis-a-vis Healthy People, AIR Joumal Section 199 (2003).

[402] AIR 1999 SC 495.

would have been infected with the dreadful disease if marriage had taken place and consummated. In such a situation public disclosure of even true private facts may amount to an invasionof the right to privacy which may sometimes lead to the clash of one person's right to beinformed. The right is not absolute and may be lawfully restricted for the prevention ofcrime, disorder or rights and freedom of others. It is to be noted that the court in this case has not just laid down that the right to life includes right to privacy. The other important part of the principle is that the Right to life includes right to healthy life. It has further laid down that where there is a clash of two fundamental rights, as in the instant case, namely the appellant's right to lead a healthy life which is her fundamental right under Article 21, the right which would advance the public morality or public interest, would alone be enforced through the process of court, for the reason that moralconsiderations cannot be kept at bay.[403] The Supreme Court was of the opinion that thelife of the fiancée would be endangered by her marriage and consequent conjugal relations with the AIDS victim, and consequently she was entitled to information regarding the medical condition of the man she was to marry".

In a recent case of *Sharda* v. *Dhannpal*,[404] "the Supreme Court was confronted with the issue whether subjecting a person to a medical test be in violation of Article 21of the Constitution. The court outlined the concept of the law of privacy in India and was of the opinion that the right to privacy in terms of Article 21 of the Constitution is not an absolute right. The Supreme Court has given a potentially contrary view from theexisting policies while answering the question whether a party to the divorce can be compelled to undergo a medical examination, in order to ascertain whether she is of unsound mind. It is said to be potentially contrary, because, in the light of the facts of the case, right of a HIV positive person was not directly in issue, but can be used to ascertain their rights, because various statements and judgments regarding the right of the persons living with HIV/AIDS are relied on to come to a conclusion regarding the issues of the present case. In this case, one of the issues was whether subjecting a personto a medical test be in violation of Article 21 of the Constitution. While

[403] Ibid

[404] (2003) 4 Sec 493, per V. N. Khare, C.J. and S. B. Sinha and Dr. A. R. Lakshmanan,JJ.

answering this question, the court relied on various decisions while relying on *M. Vijaya* V. *Chairmanand Managing Director, S. C. C. Ltd.*[405] case the court highlighted those parts of the judgment which say that the power of the State to ensure public health to all, will prevailover the right to privacy of the suspected of HIV not to submit himself forcibly for medical examination. The other part of the judgments the court relied on was that under the Immoral Traffic (Prevention) Act, the sex workers can be compelled to undergo HIV/AIDS test and that under Sections 269 and 270 of the Indian Penal Code, a personcan be punished for negligent act of spreading infectious diseases, and that in these circumstances Article 20(3) of the Constitution will not be violated. The Court thus came to the conclusion that a Matrimonial Court has the power to order a person to undergo medical test, and that passing of such an order by the court would not be in violation of the right to personal liberty under Article 21 of the Constitution of India".

It is heartening to note that recently in *Mr.X* v. *Hospital Z*,[406] "the apex courthas partly overruled is earlier decision. The petitioner raised the question whether a person suffering from HIV positive contracting marriage with a willing partner after disclosing the factum of disease to that partner would be committing an offence withinthe meaning of Sections 269 and 270 of the Indian Penal Code. In other words, the clarification was sought by the petitioner that there was no bar for marriage, if the healthy spouse consented to marry after knowledge of the HIV positive status to the other spouse. The court held that the earlier decision of the court was based on the factsof the case that it was open to the hospital to reveal such information to persons relatedto the girl whom he intended to marry and she had a right to know about the HIV positivestatus of the appellant".

However, "further observations of the court to declare in general as to whether such persons were entitled to be married or not, or if they married, they would commit an offence, or whether right to marry was suspended during the period of illness, were unnecessary and uncalled for. The development is being seen as an affirmation by the highest court in the country of rights-based response to HIV/AIDS".

---

[405] AIR 2001 Andhra Pradesh 502.
[406] AIR 2003 SC 664.

"Abortion has become a very controversial and debatable issue in the modem world of today since the recent movement towards liberalization of abortion in the western countries. Before the recent movement towards liberalization of abortion in theUnited States of America and England, abortion in most countries declared illegal unlessnecessary to preserve the life of the mother. In 1867, England and some American States liberalized their statutes to allow abortion when pregnancy is caused by rape, or to prevent the birth of a deformed child.[407]
In 1973, the United States Supreme Court in *Roe* v. *Wade*[408] and *Doe* v. *Balton*[409] ruled that a woman's decision to terminate her pregnancy, at least until the fetus is viable, in a personal matter protected from State interference by her constitutional right to privacy. In effect, these two decisions legalized abortion in the United States of America".

"In 1971, India liberalized its abortion law with the enactment of the Medical Termination of Pregnancy Act. With the enactment of this Act, the features of Indian abortion law have changed. In fact, the MTP Act, has been modelled on English Abortion Act of 1967. It provides for termination of pregnancy by a registered practitioner acting in good faith under the following circumstances:

a) where the continuance of the pregnancy would involve a risk to the life of the pregnant woman or of grave injury to her physical and mental health;
b) where there is a substantial risk that if the child was born, it would suffer from such physical or mental abnormalities as to be seriously handicapped;
c) where the pregnancy results from rape; and
d) where the pregnancy has occurred as a result of the failure of a contraceptive device or method (in this case, the anguish caused by suchunwanted pregnancy may be presumed to constitute a grave threat to mental health of the pregnant woman).

---

[407] James George, The Evolving Law of Abortion, 23 Case W. Res. L Rev. 708; 732-49 (1972); MohrJames, Abortion in America: The Origin and Evolution of National Policy, (1978).
[408] 410 US 113 (1973).
[409] 410 US 179 (1973).

The Constitution of India further liberalized the Act by an Amendment in 1975. A woman is now competent to terminate pregnancy without the consent of even her husband. Only the consent of pregnant woman is mandatory.[410] The Constitution of India guarantees right to life and personal liberty to all which implies that even the unborn child has the right to life under Article 21. Females however, argue that the choice to rear and bear children or not belongs to the woman concerned if Article 21 asto have any meaning for them. The State has enacted Pre-Natal Diagnostic Techniques(Regulations and Prevention of Misuse) Act, 1994. The Act has been strictly enforced in order to stop female feticide. The Act has made registration of Ultra Sound and othersex diagnostic techniques compulsory and the prenatal sex determination has been madea punishable offence. In our patrilineal society, desire to have son has created this complex problem forcing the females to kill the female fetus. Hence, it is submitted that once the woman enters the marriage relation, her right to privacy must be seen in the context of family life. Therefore, the father's participation in the abortion decision isnecessary to protect stability in family life, and after viability that State should prohibitto protect the life of the unborn child, except when abortion is needed to preserve the life of the mother or to protect her health when it is threatened by a substantial risk if the pregnancy is allowed to continue".

Right to Information and Right to Privacy

Right to information is a democratic right of a citizen and a part of the freedom of speech and expression. "It ensures transparency, accountability and good governancein the public system. In *Union of India* v. *Association for Democratic Reforms and Another*,[411] the Supreme Court held that citizens' freedom of speech and expression includes the right to know about the backgrounds of candidates for public office. It would be helpful for the voter to choose the right candidate. It was directed that each candidate must submit an affidavit regarding the information of his/her criminal antecedents; assets (both movable and immovable)

[410] The consent of the woman alone is required if she is above 18 years of age, but if she is a minor or alunatic, consent of the guardian is necessary.

[411] AIR 2002 SC 2112

of self and those of spouses and dependents as well; and qualifications at the time of filing his/her nomination papers forelection to the Lok Sabha, the Rajya Sabha and the State Legislative Assemblies. The Apex Court again in *PUCL* v. *Union of India*[412] guarded the citizen's right to know theantecedents about his or her candidate in election".

Thereafter, "Right to Information Act of 2005 was enacted for satisfying the people's right to know about the public information. But the right to information is notabsolute. There are two specific provisions under Right to Information Act 2005 i.e. section 8(1)(j)[413] and section 11[414], which protect 'right to privacy'

---

[412] AIR 2003 SC 2363

[413] Section 8(1)(j) of The Right to Information Act, 2005, It provides as follows:
(1) Notwithstanding anything contained in this Act, there shall be no obligation to give any citizen-
information which relates to personal information the disclosure of which has no relationship to any public activity or interest, or which would cause unwarranted invasion of the privacy of the individual unless the Central Public Information Officer or the State Public Information Officer or the appellate authority, as the case may be, is satisfied that the larger public interest justifies the disclosure of such information: Provided that the information which cannot be denied to the Parliament or a State Legislatureshall not be denied to any person.

[414] Section 11, of The Right to Information Act, 2005, It provides as follows: Third party information- (1)Where a Central Public Information Officer or a State Public Information Officer, as the case may be,intends to disclose any information or record, or part thereof on a request made under this Act, whichrelates to or has been supplied by a third party and has been treated as confidential by that third party, theCentral Public Information Officer or State Public Information Officer, as the case may be, shall, withinfive days from the receipt of the request, give a written notice to such third party of the request and of the fact that the Central Public Information Officer or State Public Information Officer, as the case may be, intends to disclose the information or record, or part thereof, and invite the third party to make a submission in writing or orally, regarding whether the information should be disclosed, and such submission of the third party shall be kept in view while taking a decision about disclosure of information: Provided that except in the case of trade or commercial secrets protected by law, disclosure may be allowed if the public interest in disclosure outweighs in importance any possible harm or injury to the interests of such third party. (2) Where a notice is served by the Central Public Information Officer or State Public Information Officer, as the case may be, under sub- section (1) to a third party in respect of any information or record or part thereof, the third party shall, within ten days from the date of receipt ofsuch notice, be given the opportunity to make representation against the proposed disclosure. (3) Notwithstanding anything contained in section 7, the Central Public Information Officer or State Public Information Officer, as the case may be, shall, within forty days after receipt of the request under section 6, if the third party has been given an opportunity to make representation under sub- section (2), make a decision as to whether or not to disclose the information or record or part thereof and give in writing the notice of his decision to the third party. (4) A notice given under sub- section (3) shall include a statementthat the third party to whom the notice is given is entitled to prefer an appeal under section 19 against thedecision.

of both private individual as well as of public official. Section 8(1)(j) of RTI Act provides that the 'personal information' does not mean information relating to the information seeker, butabout a third party. This is the reason why the Section states 'unwarranted invasion of the privacy of the individual.' If one were to seek information about himself or his owncase, the question of invasion of privacy of his own self does not arise. If one were to ask information about a third party and if it were to invade the privacy of the individual,the information seeker can be denied the information on the ground that disclosure would invade the privacy of a third party. Therefore, when a citizen seeks information about his own case and as long as the information sought is not exempt in terms of otherprovisions of Section 8 of RTI Act, this Section cannot be applied to deny the information.[415] Full Bench of the Central Information Commission in *G.R. Rawal* v. *Director General of Income Tax (Investigation)*[416] held that the payment of tax by a person was considered to be his personal matter. Unless public interest is not involved,it cannot be disclosed. In *Vijay Prakash* v. *Union of India*,[417] the Delhi High Court heldthat if the information relates to a third party and its disclosure has nothing to do with the public interest, such information would not be revealed to anyone. According to thejudgment, information (when relevant authorities prove the damage) related to the security of State, investigation, sensitive cabinet deliberations, personal data of citizens and artificial or juristic entities, etc. cannot be revealed. The Court held that the law of confidentiality and right to privacy protect individuals' personal data".

In this case, "the court also felt the practical difficulties in differentiating public and private details of the public servants. For this, the Delhi High Court said that a distinction must be made between 'official' information inherent to the

---

[415] Shri Rakesh Kumar Singh v. Lok Sabha Secretariat, Complaint No. CIC/WB/C2006/00223; Appeal Nos. CIC/WB/A/2006/00469; & 00394; Appeal Nos. CIC/OK/A/2006/00266/00058/00066/00315, Availableat:http://www.rti.india.gov.in/cic_decisions/CIC_WB_C_2006_00223, CIC_WB_A_2006 _00469,_00394, CIC_OK_A_2006_00266,_00058,_00066,_00315_M_55430.pdf (last visited on December 20, 2022 at 03.21pm).

[416] Appeal No. CIC/AT/A/2007/00490 available at: http://www.rti.india.gov.in/cic_decisions/Decision_ 05032008_01.pdf (last visited on December 21, 2022 at 09.40pm).

[417] AIR 2010 Del. 7

position and those that are not, and therefore affect only public official's private life. If public accessto the personal details such as identity particulars of public servants, i.e. details such astheir dates of birth, personal identification numbers, or other personal information furnished to public agencies, is requested, following considerations will be taken into account:

(i) whether the information is deemed to comprise the individual's private details, unrelated to his position in the organization, and,

(i) whether the disclosure of the personal information is with the aim of providing knowledge of the proper performance of the duties and tasks assigned to the public servant in any specific case;

(ii) whether the disclosure will furnish any information required to establish accountability or transparency in the use of public resources.[418]

Finally, the court acknowledged that the degree of protection of right to privacy is greater in case of private individuals. And it can be lower in case of public servants depending on what is at stake.

In Vijay Prakash's case, the writ petitioner wanted an access to his wife's service information (she was inducted in DRDO). His contention was that being a public official, his wife is under an obligation to make proper and truthful disclosure. However,the Central Information Commission rejected his plea on the ground that it lacks any public interest, as the petitioner wanted his wife's information for the divorce proceedings only".

"The Delhi High Court in the case of Secretary General, Supreme Court of India Subhash Chandra Agarwal,[419] 2009 held that "personal information including taxreturns, medical records, etc. cannot be disclosed in view of Section 8(1)(j) of the RTI Act. The Court, however, maintained that if it can be shown that sufficient public interest is involved in disclosure, the bar (preventing disclosure) would be lifted and after duly notifying the third party (i.e. the individual concerned with the information orwhose records are sought) and after considering his views, the authority can disclose it.The Court also stated that in the case of

[418] Ibid

[419] AIR 2010 Del. 159.

private individuals, the degree of protection afforded (to their privacy) is greater; in the case of public servants, the degree of protection can be lower, depending on what is at stake. This is so because a public servant is expected to act for the public good in the discharge of his duties and is accountable for them".

"Considering the accountability of a public post, the Central Information Commission in its number of decisions has declared that Section 8(1)(j) of the RTI Actis unavailable to the public servants in the following situations:

1) Public authorities cannot deny the access to the information relating to Appointments, promotions and upgradations.
2) Documents regarding the transfer of two of his colleagues, vis-à-vis whom he felt that he had been discriminated against, have to be disclosed.
3) Details of leave taken by the public servant have to be disclosed. However, the purpose for which the leave was taken need not be given because it is exemptedunder section 8(1)(j) of the RTI Act.
4) LTC Information of officials is not personal to them, therefore, will be disclosed.
5) Rules governing salary, service matters, study leave records, Posting and transfer information of public servant can't be called 'personal information'.
6) Public officers' tour program is not personal information.
7) Personal Information sought by legal heir of the deceased employee is not exempted to him.

In the similar fashion, the Kerala High Court in the case of *Canara Bank* v. *Central Information Commission*,[420] held that the information relating to posting, transfer and promotion of clerical staff of a bank do not pertain to any fiduciary relationship of the bank with the its employees within the meaning of expression 'fiduciary' under section 8(1)(e). The court reasoned that without knowing this information, one employee cannot know his rights vis-à-vis other employees. The court further held that the disclosure of such information would not cause unwarranted invasion of privacy of the other employees in any manner insofar as that information isnot one which those employees can keep to themselves".

At the same time, "it has also been recognized that privacy will not be violated

[420] AIR 2007 Ker. 225

unless there are good and sufficient reasons to disclose, as the concerned party may suffer incalculable and irretrievable harm by unjustified disclosures. The Central Information Commission, in many other decisions has not allowed disclosure of incometax returns, PAN numbers, details filed for tax determination, bank accounts, sources offunds, partnership details, plan to run dealership etc."

From above, "it has been observed that the private individual third party enjoys greater degree of protection. Moreover, the information in respect of details of customers, and private individuals, etc., falls under the exceptions of right to information given under section 8 of the Right to Information Act. The Punjab and HighCourt said that the competitive position of the third party including an information relating to commercial confidence, trade secrets or intellectual property cannot be sought as the same is barred under Section 8(1)(d) of the RTI Act. It has been further observed that personal information and the information between the person in fiduciary relationship, is exempted from disclosure under the RTI Act.[421] In order to give reasonable protection to third party's (including both public servant as well as private individual) personal information, Section 11 of the Right to Information Act requires the concerned Public Information Officer to provide proper hearing to the third party before disclosing his or her personal information".

The Gujarat High Court in *Reliance Industries Ltd.* v. *Gujarat State Information Commission*,[422] "held that it is duty vested in the Public Information Officer to give anopportunity of personal hearing to the third party, to get his submissions, whether he treats the information should be disclosed, if the information is relating to or is suppliedby the third party".

In one of the cases, "an employee was reinstated with back wages subject to the condition that the employee was not gainfully employed anywhere. However, the employer came to know about his employment in a foreign country and, remittances made by him to the bank. When the employer requested the bank to provide details of the remittances, the bank refused to provide any

[421] Rajan Verma v. Union of India, Ministry of Finance, Banking Division, New Delhi, 2008 (2) SCC 335(P&H).

[422] AIR 2007 Guj. 203

of his details on the ground of secrecyand confidentiality. But the Division Bench of Kerala High Court favored the disclosure of financial details for protecting the bank, or persons interested, or the public, against fraud or crime".[423]

Moreover, "Public Information Officials (PIOs) must have requisite amount of knowledge regarding the provisions of section 8(1) of the RTI Act 2005. The Public Information Officer must also know that mere quoting of a clause of section 8(1) is notsufficient and it should be backed by reasonable justification. It will also be useful for public authorities, researchers, activists, and citizens to be aware of these provisions andjudgments relating to these aspects." [424]

In this context, "it is worth noting that the Report of the National Sub-Committee of Chief Information Commissioners of nine states and a Central Information Commissioner (July 2008) stated that in fulfilling their role as adjudicators and regulators, they face considerable handicap. Firstly, the suppliers of information, publicauthorities, and PIOs are not properly trained and secondly the seeker of information, the common citizen is not yet fully aware of his empowerment and the procedure for securing access of information. The sub-committee concluded that many matters need not have been brought up for adjudication at all, if well informed public information officers (PIOs) and information seekers had resolved the issue at the outset. The sub- committee recommended the need for the appropriate mechanism to bring uniformity and clarity in interpretation of the Right to Information Act (RTI) by exchange of information on case law interpretation".

In *Girish Ramchandra Deshpande* v. *Central Information Commissioner*,[425] "Central Information Commissioner denied the information pertaining to the service career of the third party to the said case and also denied the details relating to assets, liabilities, moveable and immovable properties of the third party on the ground that theinformation sought for was qualified to be personal information as defined in clause (j) of Section 8(1) of the Right to Information Act. In this case, the Supreme Court held that the orders of censure/punishment,

[423] Kattabomman Transport Corporation Ltd. v. State Bank of Travancore, AIR 1992 Kerala 351.
[424] Sudhir Naib, The Right to Information Act 2005: A Handbook, 144 (2011).
[425] (2013) 1 SCC 212.

etc. are personal information and the performanceof an employee/officer in an organization, commonly known as Annual Confidential Report cannot be disclosed unless public interest is involved. Similarly, in *R.K. Jain* v. *Union of India*,[426] the Supreme Court held that information on Annual Confidential Reports (ACRs) is personal. It was reiterated that except in cases involving overriding public interest, Annual Confidential Reports (ACRs) record of a public officer cannot be disclosed to third parties. It further held that recordings made in Annual ConfidentialReports (ACRs) constitute an integral part of Annual Confidential Reports (ACRs), which is confidential, cannot be disclosed to third parties except in case of larger publicinterest. It is also mandatory that procedure laid down in Section 11 of the Right to Information Act, should be followed properly".

In *Bihar Public Service Commission* v. *Saiyed Hussain Abbas Rizwi*,[427] the Supreme Court held:

"Certain matters, particularly in relation to appointment, are required to be dealt with great confidentiality. The information may come to knowledge of the authority as a result of disclosureby others who give that information in confidence and with complete faith, integrity and fidelity. Secrecy of such informationshall be maintained, thus, bringing it within the ambit of fiduciary capacity. Similarly, there may be cases where thedisclosure has no relationship to any public activity or interest or it may even cause unwarranted invasion of privacy of the individual. All these protections have to be given their due implementation as they spring from statutory exemptions. It is not a decision simpliciter between private interest and public interest. It is a matter where a constitutional protection is available to a person with regard to the right to privacy. Thus, the public interest has to be construed while keeping in mind the balance factor between right to privacy and right to informationwith the purpose sought to be achieved and the purpose that would be served in the larger public interest, particularly when both these rights emerge from the constitutional values under theConstitution of India".[428]

Aadhar Card with Public, Private Services and Right to Privacy

[426] (2013) 14 SCC 794
[427] (2012) 13 SCC 61
[428] Ibid

Against the mandatory linking of Aadhaar card with the State benefits and services, a petition was filed by a retired judge in the Supreme Court of India on the ground of violation of right to life and personal liberty including right to privacy. Whenthe matter was pending, the Supreme Court passed an interim order on September 23, 2013, and said:

"In the meanwhile, no person should suffer for not getting the Adhaar card inspite of the fact that some authority had issued a circular making it mandatory and when any person applies to get the Adhaar Card voluntarily, it may be checked whetherthat person is entitled for it under the law and it should not be given to any illegal immigrant".[429]

Again, "on 24th March 2014, in its interim order, the Supreme Court of India in *Unique Identification Authority of India (UIDAI)* v. *Central Bureau of Investigation (CBI)*[430] restrained the petitioner from transferring any biometric information of any person who has been allotted the Aadhaar number to any other agency without his consent in writing. It was also ordered that no person shall be deprived of any service for want of Aadhaar number in case he/she is otherwise eligible/entitled. All the authorities were directed to modify their forms/circulars/likes so as to not compulsorilyrequire the Aadhaar number in order to meet the requirement of the interim order passedby the Supreme Court in this case."

In 2015 too, "the apex court again reiterated its earlier order given in September 23, 2013 and said that the aadhaar card is not mandatory and no person should be deniedany benefits or suffer for not having aadhaar card. On August 11, 2015, the Supreme Court passed an interim order in Justice *K.S. Puttaswamy (Retd.) & Another* v. *Union of India & Other*[431] and said:

---

[429] Justice K.S.Puttaswamy (retd)& anr v. Union of India & ors., Supreme Court of India, Record of Proceedings, Writ petition (civil) no(s). 494 of 2012, Ordered on 23 September, 2013, available at: http://judis.nic.in/temp/494201232392013p.txt (last visited on November 14, 2022 at 08.32pm).

[430] SLP (Crl) 2524/2014, Supreme Court of India, Record of Proceedings available at: https://sci.gov.in/jonew/bosir/orderpdfold/1943919.pdf (visited on December 17, 2022 at 04.54pm).

[431] Writ Petition (Civil) No.494 Of 2012.

1. The Union of India shall give wide publicity in the electronic and print media including radio and television networks that it is not mandatory for a citizen to obtain an Aadhaar card;
2. The production of an Aadhaar card will not be condition for obtaining any benefits otherwise due to a citizen;
3. The Unique Identification Number or the Aadhaar card will not be used by the respondents for any purpose other than the PDS Scheme and in particular for thepurpose of distribution of foodgrains, etc. and cooking fuel, such as kerosene. The Aadhaar card may also be used for the purpose of the LPG Distribution Scheme;
4. The information about an individual obtained by the Unique Identification Authority of India while issuing an Aadhaar card shall not be used for any otherpurpose, save as above, except as may be directed by a Court for the purpose ofcriminal investigation."[432]

"Despite the court's interim orders, as the Supreme Court acknowledged, many of the government agencies insist upon aadhaar card. Before providing their services, both public and private agencies ask for the aadhaar card in such a manner that the needyusers believe that the demand is not optional but mandatory one. The government submitted before the Supreme Court that it has already issued Aadhaar cards to about 90% of the Indian population. However, it does not mean that the whole 90% people submitted their biometric information voluntarily. Unhealthy socio-economic conditions of the significant population of Indian citizens affect their informed consent.Many believe that they would be denied for their eligible entitlements if they do not hold aadhar card".

"In the meanwhile, the government contended before the Supreme Court that according to the two larger bench Supreme Court's decisions of M.P. Sharma (Bench of 8 Judges) and Kharak Singh (Six Judges), the right to privacy is not a fundamental right. And subsequent judgments recognizing right to privacy are given by the smaller benches of the Supreme Court of India. The government said

[432] Writ Petition (Civil) No.494 Of 2012, In The Supreme Court of India, Civil Original Jurisdiction, ordered on August 11, 2015, available at https://sci.gov.in/jonew/judis/42841.pdf (last visited on December 09, 2022 at 05.32pm).

that the issue whether rightto privacy is fundamental right or not, should be settled first. On request, the Supreme Court referred the matter to its five judges Bench to decide the question on August 11, 2015".

"Immediately after such reference, certain applications for modification of the above-mentioned order dated August 11, 2015 were filed by the Union of India before the Supreme Court."

On October 15, 2015, five Judges Bench of the Supreme Court ofIndia (CJI H.L. Dattu, Justices M.Y. Eqbal, C. Nagappan, Arun Mishra, and Amitava Roy) modified the order in the following words:[433]

"After hearing the learned Attorney General for India and otherlearned senior counsels, we are of the view that in paragraph 3 of the Order dated August 11, 2015, if we add, apart from the other two Schemes, namely, PDS Scheme and the LPG Distribution Scheme, the Schemes like The Mahatma Gandhi National Rural Employment Guarantee Scheme 12 (MGNREGS), National Social Assistance Programme (Old AgePensions, Widow Pensions, Disability Pensions) Prime Minister Jan Dhan Yojana (PMJDY) and Employees' Provident Fund Organisation (EPFO) for the present, it would not dilute earlier order passed by this Court. Therefore, we nowinclude the aforesaid Schemes apart from the other two Schemesthat this Court has permitted in its earlier order dated August 11, 2015. We impress upon the Union of India that it shall strictly follow all the earlier orders passed by this Court commencing from September 23, 2013. We will also make it clear that the Aadhaar card Scheme is purely voluntary and it cannot be made mandatory till the matter is finally decided by this Court one way or the other".

Therefore, "the use of Aadhaar was permitted for some more governmentschemes by the Supreme Court of India. The Supreme Court also requested the Chief Justice of India to constitute a Bench for final hearing of these matters at the

[433] Writ Petition (Civil) No.494 Of 2012, In The Supreme Court of India, Civil Original Jurisdiction, Record of Proceedings, ordered on October 15, 2015, available at https://www.supremecourt.gov.in/ jonew/ropor/rop/all/389939.pdf (last visited on December 20, 2022 at 09.10pm).

earliest".

However, "the collective interpretation of the Supreme Court's three things- directing the government not to make Aadhar card mandatory, permitting the government to use it for government schemes and Aadhaar card Scheme is purely voluntary and it cannot be made mandatory till the matter is finally decided by this Courtone way or the other- are confusing in nature. On the one side the Supreme Court itselfacknowledged the fact that despite its order, public and private agencies are asking for Aadhar card from its users as if it is mandatory, and it is clear that the matter relating toAadhar card linkage is pending before the court because it involves serious privacy issues. On the other hand, the government was permitted to use the Aadhar card for anypublic scheme. It has been observed that significant percentage of population in India has submitted their biometric information under compelling circumstances, whichcannot be termed as informed consent. The government is holding the strong position under such circumstances and taking undue advantage of it".

On July 18, 2017,[434] "the five-judge Bench (comprising Chief Justice J.S. Khehar, Justices J Chelameswar, SA Bobde, DY Chandrachud and S Abdul Nazeer) decided to set up a nine-judge Bench to determine whether right to privacy can be declared as a fundamental right under the Indian Constitution. The court listed the matterbefore the Nine-Judge Constitution Bench on 19th July, 2017".

[434] Writ Petition (Civil) No.494 Of 2012, In The Supreme Court of India, Civil Original Jurisdiction, Record of Proceedings, ordered on July 18, 2017, available at: https://www.supremecourt.gov.in/ supreme court/2012/35071/35071_2012_Order_18-Jul-2017.pdf (visited on December 12, 2020 at12.11pm). The Court ordered: During the course of the hearing today, it seems that it has become essentialfor us to determine whether there is any fundamental right of privacy under the Indian Constitution. Thedetermination of this question would essentially entail whether the decision recorded by this Court in M.P. Sharma and Ors. v. Satish Chandra, District Magistrate, Delhi and Ors. - 1950 SCR 1077 by an eight-Judge Constitution Bench, and also, in Kharak Singh v. The State of U.P. and Ors. - 1962 (1) SCR332 by a six-Judge Constitution Bench, that there is no such fundamental right, is the correct expression of the constitutional position. Before dealing with the matter any further, we are of the view that the issuenoticed hereinabove deserves to be placed before the nine-Judge Constitution Bench. List these matters before the Nine-Judge Constitution Bench on 19.07.2017.

On June 9, 2017, "the Supreme Court in *Binoy Viswam* v. *Union of India*,[435] held that Section 139AA is not violative of Article 19(1)(g) of the Constitution insofar as it mandates giving of Aadhaar enrolment number for applying Permanent Account Number (PAN) cards in the income tax returns or notified Aadhaar enrolment number to the designated authorities".

On August 24, 2017, "the 9 Judges Bench of Supreme Court, which was constituted to determine whether right to privacy can be declared as a fundamental rightunder the Indian Constitution and, where the matter was listed on 19th July, 2017, gaveits unanimous decision in *K.S. Puttaswami* v. *Union of India.*[436] In this judgment, the Supreme Court declared that right to privacy is protected as an intrinsic part of the rightto life and personal liberty under Article 21 and as a part of the freedoms guaranteed byPart III of the Constitution. The Court held that the decision in M P Sharma which holdsthat the right to privacy is not protected by the Constitution stands over-ruled. The courtoverruled Kharak Singh's decision to the extent it did not recognize the right to privacyunder the Indian Constitution. The court finally clarified that the decisions recognizingright to privacy as a fundamental right (which were decided in post-Kharak Singh time) lay down the correct position in law".

On December 15, 2017, "five Judges Bench of the Supreme Court in *K.S. Puttaswami* v. *Union of India*[437] passed an interim order whereby the date for linking Aadhar card with bank accounts and mobile phones was extended to March 31st, 2018.The court also clarified that the provisions of Section 139 AA of the Income Tax Act, 1961 will be governed by the judgment of *Binoy*

---

[435] 2017 SCC Online SC 647

[436] writ petition (civil) no 494 of 2012, Decided: 24 August 2017

[437] Writ Petition (Civil) No.494 Of 2012, in the Supreme Court of India, Civil Original Jurisdiction, Record of Proceedings, ordered on December 15, 2017, available at: https://www.supremecourt.gov.in/ supremecourt/2012/35071/35071_2012_Order_15-Dec-2017.pdf (visited on December 13, 2023 at 12.18am). The court ordered: In terms of (iii) above, subject to the submission of the details in regard to the filing of an application for an Aadhaar card and the furnishing of the application number to the account opening bank, we likewise extend the last date for the completionof the process of Aadhaar linking of new bank accounts to 31 March 2018. In terms of (iv) above we extend the date for the completion of the E-KYC process in respect of mobile phone subscribers until 31March 2018

Viswam v. *Union of India*.[438] It meanslinking of Aadhar card with Permanent Account Number (PAN) is mandatory".

However, on March 13, 2018, "the Supreme Court of India in K.S. Puttaswami case extended indefinitely the March 31, 2018 deadline for mandatory linking of Aadhaar with bank accounts and mobile phones. The Supreme Court said that its interimorder on not insisting Aadhaar, except for giving subsidy, will remain in force till the five-judge bench gives its judgment on petitions challenging the constitutional validity of Aadhaar. The Supreme Court also said that the government cannot insist for mandatory Aadhaar even for issuance of Tatkal passport".[439]

In 2017, "a petitioner filed a writ petition in the Supreme Court of India, *Lok niti Foundation* v. *Union of India*[440], and prayed that the 100% verification of all the mobilephone subscribers should be done. It was argued by the petitioner that identity of each mobile phone subscriber, including his/her address, should be verified, in order to prevent criminal activities and terrorism. Replying to the prayer, the Union governmentsubmitted that the linking of the mobile phones with Aadhar card would ensure 100% verification of the identity of the mobile phone subscriber. The government promised the court to link Aadhar card of all the subscribers with their mobile phone numbers within one year". The Court said:

"In view of the factual position brought to our notice during the course of hearing, we are satisfied, that the prayers made in the writ petition have been substantially dealt with, and an effective process has been evolved to ensure

---

[438] 2017 SCC OnLine SC 647

[439] Writ Petition (Civil) No.494 Of 2012, in the Supreme Court of India, Civil Original Jurisdiction, Record of Proceedings, ordered on December 15, 2017, available at: https://www.supremecourt.gov.in/ supremecourt/2012/35071/35071_2012_Order_15-Dec-2017.pdf (visited on December 13, 2020 at 12.18am). The Court ordered: We direct that the interim order passed on 15.12.2022 shall stand extended till the matter is finally heard and the judgment is pronounced. The Court ordered: It is also directed that the same shall also control and govern the Passports (1st Amendment) Rules, 2018.

[440] Lokniti Foundation v. Union of India, Civil Original Jurisdiction, Writ Petition (C)No.607 Of 2016, Supreme Court of India, ordered on February 6, 2017, available at: http://www.sci.gov.in/jonew/bosir/ orderpdf/2857404.pdf (visited on December 23, 2022, at 02.11am).

identity verification, as well as, the addresses of all mobile phone subscribers for new subscribers. In the near future, and more particularly, within one year from today, a similar verification will be completed, in the case of existing subscribers. Whilecomplimenting the petitioner for filing the instant petition, we dispose of the same with the hope and expectation, that the undertaking given to this Court, will be takenseriously, and will be given effect to, as soon as possible".

On March 23, 2017, "the Union government issued a circular[441] imposing duty on the telecom service providers to link their pre-paid and post-paid subscribers' mobilenumbers with Aadhar card. The government relied on the Supreme Court's judgment in *Lok niti Foundation* v. *Union of India*.[442] However, on 25th April 2018, the Supreme Court, in the pending petition, clarified that the Union government misinterpreted Lokniti Foundation judgment. The court said that the Supreme Court in Lokniti judgment didn't direct anyone to link Aadhar with the mobile numbers".

On 26th September, 2018, "the Supreme Court in *Justice K.S. Puttaswamy (Retd) & Anr.* v. *Union of India*[443] held that the government's Aadhaar scheme is 'constitutionally valid' but struck down the provisions of the Aadhaar legislation linkingunique identification number with bank accounts, mobile phones and school admissions.The court said that Aadhaar Act meets the concept of Limited Government, Good Governance and Constitutional Trust".

"Restrictions or prohibitions on one's right to marriage are unconstitutional. Marriage is a part and parcel of right to personal autonomy under Article 21 of the Indian Constitution. The Supreme Court in *Lata Singh* v. *State of Uttar Pradesh,*[444] held that

---

[441] "Circular," available at: http://dot.gov.in/sites/default/files/Re-verification%20instructions%2023.03.2017.pdf ? Visited on December 23, 2022 at 02.11am.

[442] Lokniti Foundation v. Union of India, Civil Original Jurisdiction, Writ Petition (C)No.607 Of 2016,Supreme Court of India, ordered on February 6, 2023.

[443] Writ Petition (Civil) No. 494 Of 2012, Civil Original Jurisdiction of the Supreme Court of India, decided on September 26, 2018, available at: https://www.supremecourtofindia.nic.in/supremecourt/ 2012/35071/35071_2012_Judgement_26-Sep-2018.pdf (last visited on December 25, 2022, at 11.09pm).

[444] AIR 2006 SC 2522.

amajor person has freedom to any person of his own choice in the free and democratic society. The Supreme Court held that killing an individual in the name of so called 'honour' is barbaric and shameful act of murder. The Court directed the government to provide full protection the couples from any kind of societal threat. The Supreme Court of India in *Arumugam Servai* v. *State of Tamil Nadu,*[445] declared the institutions encouraging honour killings as unconstitutional. The court also warned the police officials who help the wrongdoers in honour killings. The court in *Bhagwan Dass* v. *State (NCT of Delhi),*[446] held that the case of perpetrators of honour killings falls under the 'rarest of rare cases' category, therefore, they deserve death sentence".

In *S. Khusboo* v. *Kanniammal,*[447] "the Supreme Court acknowledged that live- in-relationships come within the free expressions of an individual. It is part of one's personal autonomy. Any persecution of an individual for his or her statements favouring live-in relationship is unconstitutional, as violative of the individual's freedom of speech and expression. Same-sex marriage is also a part of an individual's right to personal autonomy. A sexual intercourse, among two adults with informed consent in their private place, does not affect any moral or public interest. It is purely a personal matter. Neither State nor society has anything to do with it".

"The High Court of Delhi in *Naz Foundation* v. *Government of NCT of Delhi*[448] declared that Section 377 of the Indian Penal Code, 1860 (IPC), insofar it criminalizes consensual sexual acts of adults in private, is violative of Articles 21, 14 and 15 of the Constitution. But the Supreme Court of India in the case of *Suresh Kumar Koushal* v. *NAZ Foundation and others,*[449] held that Section 377 IPC does not suffer from the vice of unconstitutionality and the declaration made by the Division Bench of the High court is legally unsustainable. The Supreme Court reasoned that the impugned provision cannot be declared unconstitutional because of the following reasons: The number of LGBT members in India, against the whole population, is very small.[450]

---

[445] (2011) 6 SCC 405.
[446] (2011) 6 SCC 396.
[447] 2010 5 SCC 600
[448] 2010 Cri.LJ 94 (Del.).
[449] (2014) 1 SCC 1.
[450] Ibid. The Court said: The Division Bench of the High Court overlooked that a miniscule fraction of the country's population constitutes lesbians, gays, bisexuals or transgenders and in last morethan 150 years less than 200 persons have been prosecuted (as per the reported orders) for committing offence under Section 377 IPC and this cannot be made sound basis for declaring that section ultra

1. The number of prosecutions for committing the offence under Section 377 of the Indian Penal Code is also very small.
2. Foreign judgments recognizing the so-called rights of LGBT persons, including right to privacy, autonomy and dignity, cannot be applied blindfolded fordeciding the constitutionality of the law enacted by the Indian Legislature".[451]

"The court finally said that the competent legislature is free to consider the desirability and propriety of deleting Section 377 IPC from the statute book or amend the same as per the suggestion made by the Attorney General".

But "the Supreme Court accepted the curative petition and sent the matter to thelarger bench to review Suresh Koushal decision again. The curative petition was accepted because the LGBT communities were not heard properly in Suresh Koushal judgment. Finally, in *Navtej Singh Johar* v. *Union of. India*,[452] the Supreme Court held that LGBTIQ (lesbian, gay, bisexual, transgender/transsexual, intersex and queer/questioning) people have human dignity to choose their sexual orientation and life partner. The Court said that Section 377 is against the spirit of the Indian Constitution. The Court held that the societal morality or majoritarian view or popular perception cannot override the Constitutional Morality".

It is important to mention that the "Supreme Court in *NALSA* v. *Union of India*,[453] recognized the fundamental rights of the transgenders. The Court acknowledged the fact they are being discriminated and excluded in the society. The Court described them as socially and educationally backward classes, and directed the government to provide them reservation in jobs and take positive measures for raising their standards of living so that they can live dignified lives. The court held that they have a right to be considered as third gender".

---

viresthe provisions of Articles 14, 15 and 21 of the Constitution.

[451] Ibid. The court said: In its anxiety to protect the so-called rights of LGBT persons and to declare that Section 377 IPC violates the right to privacy, autonomy and dignity, the High Court has extensively relied upon the judgments of other jurisdictions. Though these judgments shed considerable light on various aspects of this right and are informative in relation to the plight of sexual minorities, wefeel that they cannot be applied blindfolded for deciding the constitutionality of the law enacted by the Indian Legislature.

[452] (2018) 1 SCC 791

[453] AIR 2014 SC 1863

"Although Section 377 of the Indian Penal Code was not declared unconstitutional (because this issue is already pending before the larger bench), the Supreme Court in *K.S. Puttaswami* v. *Union of India*[454] argued that the Court's reasoning for validating the impugned provision in Suresh Kaushal is completely wrong.In K.S. Puttaswami's case, the Supreme Court said that the constitutional rights shouldbe protected even if the majority of population is against them. The Court observed thatthe State should protect the minorities who face discrimination in a society because theirviews, beliefs or ways of life are not accord with the 'mainstream'. Therefore, denyingright to privacy, because the population of LGBT persons is very small against the whole of India's population, is not sound and reasonable. The Supreme Court also criticized the Suresh Kaushal judgments on use of the words of 'so-called rights' relating to the LGBT persons. The Supreme Court said that LGBT rights are not illusory rights. Theseare real rights, which are based upon constitutional principles. LGBT rights are part of right to life and right to privacy. The Court insisted on the fact that Sexual orientation is an essential component of identity, which should be protected from any kind of discrimination". On the reasoning of only two hundred prosecutions for committing the offence under section 377 IPC, the Supreme Court in K.S. Puttaswami's case.

Besides, "right to have control over bodily privacy is indispensable part of rightto personal autonomy under Article 21 of the Indian Constitution. The provision relatingto the punishment for attempt to commit suicide, i.e. Section 309 of the Indian Penal Code 1860, was declared unconstitutional by the Supreme Court in the case of *P. Rathinam* v. *Union of India*.[455] The court called the impugned provision unreasonable and irrational as it aggravates the suffering of person who is already passing through some kind of mental agony. The court said that suicide or attempt to commit it causes no harm to others, because of which State's interference with the personal liberty of thepersons concerned is not called for. Therefore, the Court held that Section 309 violatesArticle 21".

But the Supreme Court's larger bench overruled P.Rathinam's verdict in *Smt Gian Kaur* v. *State of Punjab.*[456] The Supreme Court held that right to die is not part of right to life.

[454] (2017) 10 SCC 1
[455] AIR 1994 SC 1844.
[456] AIR 1996 SC 946.

"As per under existing law in India, an individual's attempt to take away his lifeis punishable. And any person, including doctor, assists him or her to commit suicide can also be punished for the offence of abetment".

However, the Supreme Court has given big relief to the terminally ill patients byallowing them to remove life supporting devices and die naturally. This is called passive euthanasia. In *Aruna Ramchandra Shanbaug* v. *Union of India*,[457] the Supreme Court legalized passive euthanasia as a part of right to life under the Indian Constitution. In the absence of any Parliamentary legislation, the court laid down guidelines for withdrawing life support devices of a patient who is in permanent vegetative state. According to the guidelines, an application can be filed by the near relatives or next friend or the doctors/hospital staff before the concerned High Court under Article 226 for withdrawing the life support devices. The High Court will monitor the whole process, and pass the appropriate orders after considering the reports submitted by the panel of doctors.

[457] AIR 2011 SC 1290.

Chapter-10

Conclusion and Suggestions

Conclusion

Privacy is an aesthetically partial theory. It varies by era, historical context, cultural status, and dominant judicial philosophy. Thus, the question "what is privacy" remains an issue for those who have tried to define it, and some researchers have abandoned their efforts to define it. Therefore, the concept of privacy does not lead toa reasonable definition. The difficulty arises from the fact that it is not a singleconcept, but a multidimensional concept that deserves to be listed rather than defined.

There is no legal and philosophical consensus on the definition of privacy. In the etymological sense, privacy is taken from the Latin term "Privatus" which means "separation from rest", deprived of something, participation in government and “privacy” meaning “deprivation” is the right to privacy which is the ability of an individual or group to isolate themselves or information about themselves and thus become selective. Privacy is about human dignity and freedom. It has long become an indispensable and inviolable part of human life. Initially, it was very narrow in scope, considered to include only "the right to be and to be much less." Later, the growing degree of maturity of democratic systems quickly came to privacy, covering many aspects such as freedom of thought, control over the body, identity, loneliness at home, control personal information.

The origins of privacy can be traced back to an article written by Warren and Brandy published in the "Harvard Law Review" in 1890, in which the concept of secrecy was first discussed in detail. The concept was first proposed in December1890, in an essay in the Harvard Law Review. They wrote, "Instant photos and a newspaper business," "intruded on sacred areas of private and domestic life."

Essentially, a few researchers discover right to privacy in 'dignity' clause of the Introduction of the Constitution of India. Be that as it may, the substance and degree of this right isn't still clear. To begin with, characterizing right of privacy is

exceptionally troublesome. It is continuously cleared out to be decided by the court, or in other words, privacy implies what the court says it is. The protection of privacy under human dignity revered under Article 21 isn't adequate to incorporate all perspectives of privacy.

Further in "most of the cases of privacy in India are also connected to police surveillance or marital rights, sexual independence, freedom of press, phone-tapping individuals. So, the area of privacy which is regularly addressed some time recently the court is restricted. Privacy is, advance an exuding right under the certain constitutional provisions. For this reason, it cannot go past the specific Article or Provision it exudes. Now and then, the confinement forced on specific provision may not be sensible for the limitation of privacy. One of the Articles which are regularly eluded for this right is Article 21 which is as of now overburdened with later advancements."

A number of legal provisions and case law exist in India which protect privacy of domestic. Case law uncovers that indeed a prostitute is entitled to beeducated some time recently entering into her room. "Unauthorized entry into a person's domestic for the reason of learning the privileged insights of his private life can sum to infringement of Article 8 of the European Convention on Human Rights which the United Kingdom has executed through the Human Rights Act of 1998 indeed in the event that the natural law the basic conditions for the offence of infringement of household privacy have not been met." Encourage, Indian Easement Act, 1882 give protection to a person's privacy of domestic.

In the event that privacy has any social center, it is the family, a set of insinuate connections that can thrive when adequately protected from public investigation. The family has been the extreme establishment of each civilization. It is the financial and beneficial unit of society. "It is the political and social unit of society; it is ethical unit as well. In numerous ways family is more basic than other institutions. Sociologists say that in case the family breaks up, civilization itself vanishes. Family life is ensured under a few statutes in India. No person is compelled to reveal any communication made between husband and wife. Essentially, no person is constrained to be a witness against her/his companion, father, mother, girl and child. The fundamental basis of this provision is that the affirmation of such declaration incorporates an effective propensity to disturb the peace of families and weaken the common certainty upon

which the joy of married life depends. Advance, Article 17 of the International Covenant on Civil and Political Rights, 1966 connect alia gives right of privacy of family." This Covenant is equally appropriate in India since India could be a party to the Pledge.

The restrictions and substance of what considered is private contrast among cultures and individuals, but share essential common topics. "Privacy is in some cases related to namelessness, the wish to stay unnoticed or unidentified within the public domain. When something is private to a person, it as a rule implies there's something inside them that's considered inalienably uncommon or personally sensitive. The degree to which private data is uncovered hence depends on how the open will get this data, which contrasts between places and over time." Privacy somewhat crosses security, counting for occurrence the concepts of suitable utilize, as well as protection, of data.

The right not to be subjected to unsanctioned intrusion of privacy by the government, organizations or people is portion of numerous countries' privacy laws, and in a few cases, constitutions. Nearly all nations have laws which in a few ways restrain privacy; a case of this would be law concerning taxation, which ordinarily requires the sharing of information around individual income or profit. In a fewnations person privacy may strife with freedom of speech laws and a few laws may require public divulgence of information which would be considered private in other nations and societies.

Privacy may be deliberately yielded, regularly in trade for seen benefits and exceptionally frequently with particular perils and misfortunes, in spite of the fact that typically an awfully key view of human connections. Scholastics who are financial specialists, developmental theorists, and investigate psychologists portray uncovering privacy as a 'voluntary sacrifice', for occasion by willing members in sweepstakes or competitions. Within the trade world, an individual may volunteer individual subtle elements (frequently for publicizing purposes) in arrange to bet on winning a prize. Personal information which is deliberately shared but along these lines stolen orabused can lead to identity theft.

Privacy, as the term is for the most part caught on within the West, isn't a universal concept and remained for all intents and purposes obscure in a few societies until later times. Most societies, in any case, recognize the capacity of individuals to withhold certain parts of their personal information from more extensive society - a figleaf over

the privates being an old illustration. The right of privacy has been pickingup acknowledgment, in spite of the fact that recently, and it has been pronounced as a part of Article 21 in spite of the fact that the Indian Constitution does not talk in express terms. The right to privacy can be worked out as it were in case the violator is the state and not a private person or institution. This right being not outright can be obstruction within the intrigued of wellbeing. This right doesnot deny any distribution of matter which is of common intrigued.

So distant the law relating to the right to privacy has been consigned to a penumbral status and is still going through the state of earliest stages. It is high time that the government and information technology industry come together to check out ways and implies to check the issue of intrusion of privacy. Our legislatures got to protect privacy instead of laws that encourage infringement of individual's privacy within the title of administrative capacities.

"Privacy is a fundamental human right recognized in the United Nation Declaration of Human Rights, the International Covenant on Civil and Political Rights and in many other international and regional treaties. Privacy underpins human dignity and other key values such as freedom of association and freedom of speech. It has become one of the most important human rights issues of the modem age. The growing importance, diversity and complexity of this fundamental right are reflected. However, the right to privacy is under serious threat due to the emergence of information technology. The application of various electronic gadgets has made the surveillance of the activities of the individuals very easy. The existing laws have been found to be ineffective in dealing with this problem and this has necessitated enactment of new laws."

About each nation within "the world recognizes a right of privacy expressly in its Constitution. At a least, these provisions incorporate rights of sacredness of the home and secrecy of communications. Most recently-written Constitutions such as South Africa's and Hungary's incorporate particular rights to access and control one's personal information. In numerous of the countries where privacy isn't unequivocally recognized within the Constitution, such as the United States, Ireland and India, the courts have found that right in other provisions. In many nations, universal agreements that recognize privacy rights such as the International Covenant on Civil and Political Rights

or the European Convention on Human Rights have been embraced into law."

Within the early 1970s, nations started embracing wide laws aiming to protect person privacy. Throughout the world, there's a common development towards the appropriation of comprehensive privacy laws that set a system for protection. Most of these laws are based on the models presented by the Organization for Economic Cooperation and Development and the Council of Europe.

In 1995, "cognizant both of the deficiencies of law, and the numerous contrasts within the level of protection in each of its States, the European Union passed a Europe-wide order which can give citizens with a more extensive extend of protections over mishandle of their data. The mandate on the "Protection of People with respect to the preparing of personal data and on the free development of such data" sets a benchmark for national law. Each EU State had to pass complementary enactment by October 1998. This prerequisite has brought about in developing weight exterior Europe for the entry of privacy laws. More than forty nations presently have data protection or information privacy laws. More are within the handle of being ordered."

Data protection is an issue that is gaining increasing importance as our transnational exchange of private information grows. The evidence gathered during this study showed clearly that the success or failure of privacy and data protection is not governed by the text of legislation, but rather by the actions of those called upon toenforce the law. The stronger, results oriented approach aims to protect data subjects against personal harm resulting from the unlawful processing of any data, rather than making personal data the building block of data protection regulations.

The Indian laws remain unsatisfactory regarding stringent legislation to protect data. Though, the Data Protection Bill 2019 has been passed and it is anticipated that India will soon enact such legislation which will provide acceptable protection to private data. Unless addressed, the systemic problems of enforcement in India, and specifically, of unresolved cases due to court delays, will continue to render India'sdata protection laws inadequate. In addition, Cyber Infringement Courts, specialized courts with jurisdiction over an intellectual property and data protection issues, are a necessary solution to India's enforcement problems. India must expediently adopt this system of specialized courts in order to render adequate protection to data and maintain its

growing presence in the global technology arena.

Cloud computing has critical suggestions for the privacy of personalinformation as well as for the privacy of trade and legislative information. Within the Indian scenario, as cloud computing could be a novel concept there's no law which particularly administers it and the law at show needs clarity. Questions as to the pertinent law and the jurisdiction of the court still stay unanswered. Still, associations are exchanging from conventional strategies of storage to cloud computing since of thecost proficiency. The proposition derived here is that cloud computing may not be perfect for all associations since of the different issues raised but, it is economical and convenient for worldwide associations to utilize in arrange to store data which can be accessed from any portion of the world at any time.

After looking into a few of the "cyberspace" enactment, it isn't astounding to discover that the enactment in this field needs clarity. “The Digital Millennium Copyright Act of the United States has clearly defined the standard of knowledge an ISP is required to possess for it to be held liable for illegal third-party activities. The Digital Millennium Copyright Act allows Internet Service Providers (ISP) to terminate the accounts of individuals who infringe copyrights on a regular basis. Furthermore, inthe United States, ISPs have to register an agent with the appropriate office so they canreceive information of copyright infringements.” This eliminates the possibility of an ISP being caught unaware of third-party infringements.

As is seen, the EU Directive has a few escape clauses that have to be closed. The foremost troublesome of which incorporate, a need of a "take note and takedown" procedure, which undermines freedom of expression; and the reality that the current administration may really advance out of line competition in a few circumstances. The lack of a take note and take down procedure causes the Internet Service Providers to gotten to be a sort of censorship body, in arrange to maintain a strategic distance from liability when they select to require down a Web page upon receipt of a claim with respect to the substance on that page. This debilitates freedom of expression as long as clients are without protection against unwarranted complaints. Unjustifiable competition may be advanced in cases where companies lock in in a frame of commercial war in cyberspace, heaving awful confidence claims against their competitor's Web substance.

The Credit Information Companies (Regulation) Act 2005, “although it is not yet fully operational, includes privacy principles which cover most usual data protection rights, though only in relation to the context of credit reporting. There is otherwise as yet no significant legislation protecting personal information in India, though some provisions in the Information Technology (Amendment) Act 2008 may emerge as significant depending on regulations made and implementation, particularly concerning data security.” There is no special protection for personal information smuggled into India from other jurisdictions.

There's a successful right of access to personal data within the public segment, “under the right to Information Act 2005, and this right of access is probably the foremost noteworthy viewpoint of data protection in India at display. There's moreoverprotection inside India against telemarketing through the Telecom Unsolicited Commercial Communications Regulations 2007.” Noteworthy in spite of the fact that these regions are, it cannot be said that privacy standards apply to most perspectives ofIndian life.

The Central Information Commission(CIC), State Information Commissions (SIC), and the network of Information Officers in all public authorities in India, constitute an effective means of administering and enforcing the access principle. “The Central Information Commission actively enforces the law by the use of both compensation and penalties. If the Right to Information Act 2005 had added to it the rest of the set of data protection principles, India would be likely to have an effective enforcement system for data protection. Neither the National Human RightsCommission nor the Cyber Regulation Appellate Tribunal seems to be as promising asthe basis for a data protection authority.” The Do-Not-Call register seems to be developing effective enforcement, but that is in a much-specialized area.

The Credit Information Companies (Regulation) Act 2005, “although it does include a full set of privacy principles, is lacking in comprehensive enforcement measures. It relies almost entirely on prosecution of offences, either through the courts or administratively by the Reserve Bank. There is no obvious way for complaints to be made. The Reserve Bank has extensive directive powers, but is not a consumer protection agency and its interests are more obviously in creating a modem credit economy than in protecting consumer privacy.” However, the system is untested, and it is necessary to wait and see.

There is as yet no significant self-regulation for the purposes of privacy protection in India. “There are no aspects of India’s data protection which would unequivocally be regarded as ‘adequate’ by European Union standards as yet, though further investigation might indicate that there are some sectoral areas of adequacy. This could also change as rules are made under existing legislation. The most likely candidates (in decreasing order of likelihood) might be: The credit reporting system, but only after it has been tested in practice; The right of access (but only in relation to public authorities); The implementation of the security principle via both compensatory provisions (subject to how Section 43A is implemented) and offences; The provisions concerning opting out from direct marketing.”

“The cultural dimensions of right to privacy with reference to conventional Indian scene are quite distinctive from another western world. A tremendous larger part still lives customarily in expansive joint families. The autonomy of decision making isn't profited by a person part. The head of the family decides critical things of the family and individuals of the family are submissive to the head and they recognize his intelligence. The development of urbanization, the spurt in populace and different sorts of deficiencies caused an inconsistency within the living as a result of which the ancient life fashion seems not be supported. Liberation of women, urbanization and lacking assets have acted as catalysts to the inborn longing for privacy to bloat it up in an amplified shape that we have seen within the later times. Things have changed enormously with the social, political, scientific and industrial headways and nowadays man is declaring his right to privacy in all its dimensions.”

“It may be related to say here that the right to privacy as an independent and unmistakable concept begun within the field of tort law, wherein an illegal intrusion of privacy was recognized as a cause of activity for a remedy in harms. Privacy as a significant right includes a generally modern presence in India. The law regards the right to privacy in two separate and particular areas, which are but two sides of the same coin, private law and public law i.e., the common law of privacy that manages a tort activity for harms coming about from an illegal intrusion of privacy and the constitutional recognition given to the right of privacy which protects personal privacy against illegal government attack.”

Sexual privacy is closely associated with privacy of domestic and family. “Sex has been

a natural encourage of all the creatures of the world. Nature has soaked up this intuitive so that the process of reproduction is proceeded, and this would have been the reason for expansion of component of delight with sexual intercut. About all social orders have looked for privacy for sexual connection. Indian law secures privacy of sex indeed in brothel. Case law uncovers that indeed a woman of simple ideals merits right of privacy. A few of Indian tribe's hone polygamy either polyandry or polygyny. Indeed, in case of majority of accomplice sexual privacy is alluring. In any case, sexual privacy does not secure unnatural sexual connection." Unnatural sexual exercises conducted in private are moreover punishable in India.

Whether the right of privacy amplifies in connection to the matrimonial rights? "Whether a wife can say no to have a sexual relation with her husband? It is evident that the address of woman as a person having partitioned substance from her husband having the right to privacy against her possess husband, whereas marital bond proceeds, has pulled in legal consideration. There are diverse suppositions in this matter." Andhra Pradesh High Court in *T. Sareetha* v. *T. V. Subbaiah*,[458] received the extraordinary positive view perceiving the right to privacy. The Supreme Court of India has passed the issue of privacy in *Saroj Rani* v. *Sudershan Kumar*[459].

Law of trespass and nuisance too secure privacy intrigued. The tort of nuisance is immature in India. It does not secure adequate privacy intrigued. "It is additionally restricted as trespass; it secures from physical impedances as it were. It does not ensure photography, bugging, tapping, snooping from the separate without entering to others arrives. Prying neighbor with binoculars, electronic listening stealthily and spying by electronic gadgets don't sum to trespass. In this way, trespass ensures privacy of an individual in certain regard. It confines, physical mediation so its scope is restricted to secure privacy." Indian lawful framework ensures such sorts of privacy which is inferred out of trespass law.

Freedom of speech and expression is guaranteed by the Constitution of India. It incorporates freedom of press. "Freedom of Press has been acclaimed as the foundation of present-day law-based state. It is frequently portrayed as fourth bequest. It is far from being obviously true as to whether freedom of press is predominant to that of

[458] AIR 1983 AP 356
[459] AIR 1984 SC 1562

privacy intrigued? It changes agreeing to circumstances. Press isn't permitted to distribute any matter which is of private nature. Press is entitled to distribute as it were those things which are of authentic public intrigued. To keep the Press as a solid medium that can safeguard public interest it must observe self-censorship with a set of standards based on sound standards that offer due respect to both freedom of expression and right to privacy. The infringement by Press and other mass media into privacy rights of individuals through the assistance of modem technology is the new risk. The concept of privacy is multidimensional and ever extending with each progression in technology. Consequently, it appears that advancement of the concept step by step through judicial decisions would be a judicious course." The judiciary can take note of the ever-broadening concept and utilize it as a parameter for choosing debate that includes the address of privacy rights.

The law authorization agencies have accomplished the wide run of uncontrolled and unguided optional powers in case of avoiding any commission of offense under the "National Examination Agency Act 2008 studied with Information Technology (Amendment) Act 2008 in India. India's mass surveillance project is founded upon the Central Monitoring System Project, Defense Research and Development Organization (Network Traffic Analysis)(DRDO NETRA), Lawful Intercept And Monitoring Project, National Cyber Coordination Centre (NCCC), Telecom Enforcement Resource and Monitoring Project, National Intelligence Grid or NATGRID, and Aadhaar Biometric Identity Card. Surveillance technologies includingClosed-Circuit Television cameras (CCTV), biometric devices, Deoxyribonucleic Acid (DNA) tests, Global Positioning System (GPS) and Radio Frequency Identification (RFID) devices, computer software applications or software agents,social networking sites and drones, have enabled the law enforcement agencies to access, collect and store unlimited amount of the individuals' personal information ina clandestine manner." It implies that the government agencies' cutting-edge ways of collecting personal information around the individuals from telecom service providers, internet companies, social networking sites, app designers etc. are totally uncontrolled and untraceable, and the individuals are in no position to discover out whether they arebeing observed or not, and for what purposes their personal information is being collected and utilized by the law enforcement agencies. Since the government organizations know that the extraordinary capabilities of the surveillance technologies would not let them be

followed at any time whereas interference communication messages, they would not indeed bother to take after any procedural safeguards specified under the current legislations like Telegraph Act and Information Technology Act. It may permit the law requirement organizations to conduct any number of suspicions less looks for all legal and illegal purposes. Hence, affect and utility of modern technologies are required to be reconsidered through legitimate legislations as these have potential to attack our private lives.

The requirement for right to privacy gets to be self-evident each day. The steady governmental mediations in public life and the improvement of modern technology which makes a difference in burrowing out and checking everyone's individual undertakings make life hopeless. Presently a day, the utilize of Closed-Circuit Television cameras (CCTV) in open places, teach, private places get to be a common hone, but in dangers to privacy when such gazettes are misused. Utilizing biometric technology for surveillance of physiological and behavioral highlights of human beings once more raises genuine human rights concerns, more especially privacy interface. Taking such genuine dangers to privacy into thought, within the judgment of K.S. Puttswamy case.It was proposed that in spite of the fact that the government tries to make strong administration of data protection, such an administration requires a cautious and touchy adjust between person interface and true-blue concerns of the stat which incorporates, for occurrence, protecting national security, avoiding and exploring crime, empowering innovation and the spread of information.

Data Privacy Protection issues must be "seriously examined by the legislature. The Data Protection bill, 2019 will require a new review to ensure minimal protectionof personal data. The bill has to prove itself in the age of artificial intelligence and the new challenges in data processing. The bill creates a monopoly for state actors, dilutes property right to data and private companies around the would have a significant compliance burden. The current bill does not properly address privacy-related issues in today's technologies world. The government opens up the possibility of mass surveillance and thus encroaches on people's privacy."

New threats to privacy will always arise as modern technologies and infrastructures keep growing. "A number of problems have arisen in connection with the various aspects of privacy in modern Contemporary Society. A threat to privacyhas been

created and by formulated in such a way that it meets the needs not only of the present generation but also of the future generation. The new privacy-related issuesgive the judiciary greater powers over the right to privacy. Legal philosophy and socio-cultural norms determine the context of privacy in the country." The countries are facing new challenges in terms of privacy protection.

In the Case of "Justice K.S. Puttaswamy, the Supreme Court, through six partitioned suppositions, articulated privacy to be an unmistakable and autonomous essential right under Article 21 of the Constitution. The core of the decision spelled out a sweeping elucidation of the right to privacy it was not a contract right against physical attack, or a subordinate right under Article 21, but one that secured the body and intellect, counting decisions, choices, data and flexibility. Privacy was held to be an overarching right of Part III of the Constitution which was enforceable and multifaceted. Details regarding the scope of the right were examined within the different opinions. The Court overruled the judgments in M.P. Sharma, and Kharak Singh, insofar as the last mentioned held that the right to privacy was not a fundamental right. With concern to M.P. Sharma, the Court held that the judgment was valid for keeping up that the Indian Constitution did not contain any constrain to the laws on search and seizure analogous to the Fourth Amendment within the Joined Together States Constitution. Be that as it may, the Court held that the Fourth Amendment was not a comprehensive concept of privacy and a nonappearance of a comparable protection within the Constitution did not accomplish that there was no characteristic right to privacy in India at all – and so the conclusion in M.P. Sharma was overruled. The Court rejected the insular see of personal liberty (ordered liberty) embraced by Kharak Singh, which Justice D.Y.Chandrachud alluded to as the 'silos' approach borrowed from A.K. Gopalan. The Court observed that this approach of seeing fundamental rights in water-tight compartments was annulled after Maneka Gandhi. The Court encourage observed that he larger part supposition in Kharak Singhendured from an inner inconsistency, as there was no legitimate premise to have struck down domiciliary visits and police reconnaissance on any ground other than privacy a right which they alluded to in hypothesis but held not to be a portion of the Constitution. The Court moreover held that the decisions consequent to Kharak Singh maintaining the right to privacy were to be studied subject to the principles laid down within the judgment. The Court moreover examined the agreed case for whether the right to privacy was secured under the right

to life, personal liberty and the freedoms guaranteed under Part III of the Constitution. The Bench built up that privacy was not an elitist construct". It rejected the contention of the Attorney General that the right to privacy must be spurned within the intrigued of welfare privileges given by the state.

Essentially, "whereas holding that the right to privacy was not outright in nature, the judgment too gave an outline of the standard of judicial review that must beconnected in cases of intrusion by the State within the privacy of a person. It held that the right to privacy may be limited where such intrusion meets the three-fold necessity of legality, which hypothesizes the presence of law; need, defined in terms of agenuine state aim; and proportionality which guarantees a level-headed nexus between the objects and the implies received to attain them. Justice S.K Kaul included a fourth prong to this test which commanded 'procedural guarantees against mishandle of such interference'. At the same time, Justice J. Chelameswar held that the standard of 'compelling state interest' was as it were to be utilized in privacy claims which merit 'strict scrutiny'. As for other privacy claims, he held that the fair, reasonable and sensible standard under Article 21 would apply. Agreeing to his judgment, the application of the 'compelling state interest' standard would depend on the setting of the case. The Court too underlined the fact that sexual orientation was a basic aspect of privacy. It encourages examined the negative and positive substance of the right to privacy, where the State was not as it were controlled from committing an interruption upon the right but was moreover committed to require essential measures to protectthe privacy of an individual. The judgment held educational privacy to be a part of the right to privacy." The Court whereas noticing the require for a data protection law cleared out it within the space of Parliament to administer on the subject.

"The Aadhaar Act was propelled with the reason to donate identity and strengthening to the marginalized segment of the society. It gives a unique identification number to the citizens of India. The Aadhaar number is unique and so, it can't be copied. The unique identification guarantees that the benefits and appropriations of the Government are profited by the segment of society for which it isimplied. Aadhaar can anticipate unjustifiable hones and spillage of thousands of croresof cash. Numerous privacy rights questions were moreover raised within the case. The address of dignity of citizens, instructive self-determination and assent shaped the premise for the privacy rights claims. The right to Privacy shaped a vital portion of the case. A five-judge bench of

the Hon'ble Supreme Court on 26th September 2018, conveyed a judgment in favor of respondents. The legitimacy of Aadhaar was maintained by the Court after striking down different clauses and Areas of the Act which were opposite to the Constitution and violated the rights of the citizens. Justice A K Sikri who composed the majority of the judges announced the Aadhaar Act to be valid after striking down Section 33(2) and Section 57 of the Act. Different questions were raised by the petitioners on issues just like the Right to Privacy of the citizens and the plausibility of state observation as well as the plausibility of breach of data which was collected by the Government for Aadhaar cards of the citizens. The questions of the petitioners have moderated the claim of UIDAI that their frameworkis one of the finest within the world and secured sufficient to keep the data of the citizens secure."

The Court held the Aadhaar Act to be constitutionally substantial as the Act was beneath reasonable restrictions of the Constitution. "The majority of the honorable Bench moreover expressed that the right of choice of the citizens to profit the Aadhaar card will not be secured by maintaining the Aadhaar Act. The citizens will not be cleared out with a choice as Aadhaar will be obligatory for profiting the appropriations and benefits of the Government and on the off chance that a citizen is avoided from profiting the appropriations and benefits of the Government due to need of Aadhaar or authentication problem it can result within the infringement of the dignity of the citizen. The Bench also said that linking of Aadhaar to Pan card isn't vital as there isn'tany constitutional basis behind it. Maintaining of Aadhaar can conceivably result within the infringement of the right to Privacy indeed after striking down Section 33(2) and Section 57 of the Act. In arrange to protect the right to Privacy of thecitizens the Court clearly ruled out the plausibility for private substances to utilize the authentication component or for inquiring Aadhaar subtle elements by the citizens." The step taken by the Court was to protect the right to Privacy of the citizens and it clearly appeared that the right to Privacy is without a doubt a Fundamental Right.

The CA and Facebook scandal raised major concerns about people's privacy: "how the data of millions of Facebook users leaked and how the voter's psychological profile was created to aid Trump in the elections. The Aadhaar program in India also raised serious privacy concerns in the country. Various issues were raised such as identity theft, identity matching, illegal tracking, identification without consent; however, the Supreme Court has upheld the validity of Aadhaar's plans and concludedthat they did

not violate privacy, but relied mainly on other aspects of Article 21 that the right to privacy. Jamaica Supreme Court has overturned Jamaica's national registration and identification law based on the minority opinion of Chandrachud J. in Aadhaar's judgment. The national identity system must also be viewed from the perspective of privacy."[460]

Presently, mass surveillance projects utilizing extraordinary capabilities of the modern surveillance technologies have raised genuine issues. Such surreptitious surveillance without having solid and viable privacy protected legislation isunconstitutional. It violates the individuals' privacy rights counting freedom of speech or expression, freedom of association, freedom of religion, right to live namelessly, right to be forgotten, etc. Existing legal system isn't adequate in the event that the government agencies utilize the surveillance technologies to act discriminatorily against the innocent individuals, political dissidents, marginalized population, religious minorities, gender minorities, etc.

India is still at a very early stage of developing personal data protection, though some of the signs are promising. Balanced against this must be the increases in surveillance powers.

Last but not least, the researcher can conclude that the persistent prepare of social alter numerous modern technologies and infrastructures in our lifestyle that posture a threat to our recognized human rights and the right to privacy. The day-by-day challenges to this right lead to many new dimensions of the right to privacy, whichin turn increments lawful activism within the range of the right to privacy, which is why numerous modern cases develop, such as *AMP v. Persons Unknown*[461], *Obergefell v. Hodges*[462], *Suresh Kumar Koushal* v. *Naz Foundation*[463], *NazFoundation* v. *Government of NCT of Delhi*[464], and *Justice K.S. Puttaswamy* v. *Union of India*[465]. In this sense, the right to privacy isn't an inactive but an energetic right, and constant progress and social

[460] Ashok Kini, "Jamaican SC Quotes Justice Chandrachud's Dissent to Strike Down Aadhaar-Like Programme", The Wire, Apr. 13, 2019, available at https://thewire.in/law/jamaica-supreme-court-aadhaar-justice-chandrachud. Visited on 18 December2022 at 08.21pm.
[461] 2011 EWHC 3454 (TCC).
[462] 576 United States 644 (2015).
[463] 2014, 1 SCC 1.
[464] 2010 Cri.LJ 94 (Del.).
[465] Writ Petition (Civil) No.494 Of 2012.

development are dependable for the method of ever- growing and endless development of the right to privacy. In any case, the right to privacy may be a restricted right. Subsequently, it might never be an impediment to the organization of equity in any society.

Suggestions

On the premise of study, within the preceding chapters, the following suggestions are being submitted for end of the course of activity by the researcher -

1. The essence of Cyber Privacy lies in Awareness and Selection of information to be shared by each individual.
2. There is a need to inculcate cyber ethics. Cyber ethics means the field of inquiry dealing with ethical problems aggravated, transformed or created by computer and network technology.
3. Law strategies must include a comprehensive compliance process, management of internal privacy, employee training, awareness, self-regulatory efforts, corporate interface with privacy awareness seminars and online dispute resolution mechanism. Every corporate, private, as well as government sector must comply Information Security Management standards.
4. The internet service providers must strictly verify, upon an individual's connection or 'handshake' with the provider, that the individual user has installed. With this an unsafe or unsecured individual user would not be permitted public access to the 'information superhighway', just as an unsafe vehicle would be prohibited from driving on public thoroughfares.
5. A Comprehensive legal mechanism is needed to address various platforms of expression including law, administration and a well devised redressal mechanism.
6. It is suggested that till the parliament devises comprehensive law in this regard the Supreme Court should liberally interpret the existing laws to address the issue of privacy and devise policy guidelines to be effective till any further advancement is made by the parliament in this regard.
7. It is suggested that assembly and the courts take note of this. In India, the Constitutional provisions of phone capture attempts need the clarity and profundity

as compared to its partner United States of America. The law or wiretap in India is, therefore, satisfactory neither from the point of view of the law requirement nor the accused.

8. Another suggestion is made in regard to protection of IP Rights. Government isnot too effective in protecting the rights relating to unpublished work. Copyright and Patent law cannot cover the whole spectrum of research work. While work is still in process, no law protects from being used by some others. Any unpublished work is not protected by copyright law. Hence, there is a dire need to develop a code of conduct to those all who practice in any research work.

9. There's a critical need to control breach of online privacy and outline certain rules for protecting the same because Infringement into Right to privacy through progressed modern technology could be a present-day issue confrontedby many people.

10. There's a need for amending the Constitution to supply a specific definition of privacy. Such a law will secure the women from specific crimes which can be committed against woman as it were. The ever-increasing prodding, attack, etc. can be handled and interface of women protected when a stricter law on privacy is in its put.

11. However, in spite of the significance of these areas, till presently we need legitimate systems within the areas of data security, data protection and privacyprotection. We direly ought to define data protection law in India and privacy laws in India. At the approach level as well privacy rights and data protection rights have been overlooked in India. In reality, an Indian national privacy policy is lost till presently. Indeed, administrative endeavors in this respectare not satisfactory in India. A national privacy policy of India is direly required.

12. It is suggested that the Aadhaar should be there for conveyance of endowmentsand overseeing other government programs, but it should not change over framework into an observation State. The Aadhaar's security and privacy measures ought to be made more exacting so that identity theft is limited and other frame of imitations cannot be done.

13. The Privacy Bill does not "provide for a particular self-regulation system where

industry groups create and comply with privacy standards. An ombudsman of the sector may also be appointed for this purpose. National principles of privacy as specified in the report may be applied to harmonies laws, policies and practices, including but not limited to interception, the use of personal IDs, the use of audio and video recordings, the use of gene and body materials and the Government's and private sector's use of personal data."

14. An "enforcement system shall include setting up of the Office of Privacy, regional and central commissioners, defining their roles and co-regulations, establishing a system for complaints and redress for aggravated people, and prescribing physical protection, including the investigation and search and listing of offences, associated remedies and sanctions. The meaning of personal data should depend on the context in which the data controller is used, gathered or processed."
15. The new Data Protection "Law should comply with international responsibilities. Domestic security, public order and public disclosure, preventive action, detection, investigative action, prosecution of criminal acts, protection of individuals or of the rights and freedoms of others should be excluded from the privacy law. The national privacy principles such as notice, openness, access and rectifications, permission, liability and security, purpose restriction and collection limitation should all be tested by any legislation governing privacy."

Bibliography

Books: -

- Adams, Helen R. Bocher, Robert F. Gordon, Carrol A. and Barry-Kessler, Elizabeth., "Privacy in the 21st Century" 1st Edition, Libraries Unlimited, Westport, Connecticut, London, 2005.
- Alderman, Ellen. & Kennedy, Caroline., "The Right to Privacy" Alfred A. Knopf, New York, 1995.
- Anand, Dr. V. K., "Human Rights (Incorporating Supreme Court on Human Rights, Dr. P. K. Singh)", 2nd Edition, Allahabad Law Agency,Haryana, 2008.
- Bakshi, P. M., "Defamation and Privacy in Law of Defamation: Some Aspects", N.M. Tripathi Private Ltd., Mumbai, 1986.
- Bakshi, P.M., "The Constitution of India", 14th Edition, Universal LawPublishing, New Delhi, 2017.
- Basu, D.D., "Law of the Press" 5th Edition, LexisNexis, Nagpur, 2010.
- Basu, D.D., "Introduction to the Constitution of India" Wadhwa and Company Law Publishers, Nagpur, 2002.
- Basu, D.D., "Human Rights in Constitutional Law", 2ndEdition, Wadhwa and Company, Nagpur, 2003.
- Basu, Justice Palok.,"Law Relating to Protection of Human Rights under the Indian Constitution and Allied Laws", 2ndEdition, Modern Law Publications, New Delhi, 2007.
- Bhat, P.Ishwara., "Fundamental Rights A Study of their Interrelationship", 1st Edition, Eastern Law House Private Ltd, Lucknow, 2004.
- Blackstone, William., "Commentary of the Laws of England", Vol. I, 4th Edition, J.B. Lippincott Company, Philadelphia, 1893.

- Brown, Geoffrey., "The Information Game: Ethical Issues in a Microchip World", 1st Edition, Humanities Press International, Inc. Publication, New Jersy, U.S.A & London, U.K., 1990.
- Carey, Peter., "Media Law", 5th Edition, Sweet & Maxwell Ltd. Publication, London, 2010.
- Chandra, Dr. U., "Human Rights", 5th Edition, Allahabad Law Agency Publications, Allahabad, 2004.
- Cohen William & Danelski's David J., "Constitutional Law: Civil Liberty and individual Right" 6th Edition, Foundation Press New York, 2002.
- Davis, Howard., "Human Rights and Civil Liberties", 2nd Edition, London and New York: Routledge, Taylor & Francis Group, 2013.
- Dhirajlal, Ratanlal., "The Law of Torts", 26th Edition, Reprint 2015, Lexis Nexis Butterworths Wadhwa, Nagpur,2010.
- Dhyani, S. N., "Fundamentals of Jurisprudence: The Indian Approach", 3rd Edition, Reprint 2015, Central Law Agency, Allahabad, 2004.
- Gordia, Diwan, Madhavi., "Facets of Media Law" 2nd Edition, Eastern Book Company, Lucknow, 2013.
- Gour, H. S., "Penal Law of India", Vol I, 11th Edition, Rev. 2003, Law Publisher India Pvt. Ltd, Allahabad, 2003.
- Houston, R. F. V., "Salmond on the Law of Torts", 17th Edition, Sweet &Maxwell Ltd, London,1977.
- Huda, & Syed Shamsul., "Principles of the Law of Crimes", 1st EditionReprint, Eastern Book Company, Lucknow, 2011.
- Jain, M.P., "Indian Constitutional Law", 7th Edition, LexisNexis, Nagpur, 2014.
- Jain, M.P., "Indian Constitutional Law", 6th Edition, Reprint 2011, LexisNexis Butterworths Wadha, Nagpur, 2011.
- Jethmalani, Ram & Chopra, D. S., "Cases and material on Media Law", 1st Edition, Thomson Reuters, India, 2012.
- Joshi, K.C., "Constitutional Law of India", 3rd Edition, Central Law

- Kenny & Courtney Stanhope., "outlines of Criminal Law" 19th Edition., New Delhi Universal, 4th Indian Reprint, New Delhi, 2010.
- Kothari, C. R. and Garg, Gaurav., "Research Methodology: Methods and Techniques",4th Edition, New Age International (P) Ltd, New Delhi,2019.
- Kumar, Ravinder & Goyal, Gaura.,"The Right to Privacy in India-concept and Evolution", 1st Edition, Partridge India, India,2016.
- Lakshminath A. & M. Sridhar., "RamaswamiIyer' s The Law of Torts", 10th Edition, Lexis Nexis Butterworths, Nagpur, 2007.
- Madgwick, Ronald & Tony., "The Invasion of Privacy", 1st Edition, Pitman Publishing Corporation, New York, U.S.A., 1974.
- Millard, Christopher & Mark Ford., "Data Protection Laws of the World", Sweet and Maxwell, Vol.1, United Kingdom,2000.
- Mishra, G., "Right to Privacy in India", 1st Edition, Preeti Publications, Delhi,1994.
- Mozika, Jyoti J., "Law and Protection of Right to Privacy" First Edition, R. Cambray & Co. Pvt. Ltd., Kolkata,2013.
- Myneni, S. R., "Legal Research Methodology", 14thEdition, Reprint 2010- 2011, Allahabad Law Agency, Allahabad, 2009.
- Narayana, P. S., "Law of Injunction" 1stEdition, Asia Law House, Allahabad, 1988.
- Nigam, R.C., "Law of Crimes in India", Vol. I, 36. Asia Publishing House, Delhi,1965.
- Noorda, Catrien. & Hanloser, Stefan., "E-Discovery and Data Privacy: A Practical Guide", Wolters Kluwer Law & Business Publication, Netherland, 2011.
- Pandey, J.N., "Constitutional law of India", 54th Edition, Central Law Agency, Allahabad, 2017.
- Pandey, K.A.,"B. M. Gandhi's Indian Penal Code", 4th Edition, p CXLII. Eastern Book Company, Lucknow, 2017.
- Pillai, PSA., "Criminal Law", 9th Edition, Lexis Butterworths, New Delhi,

- Pylee, M. V., “Select Constitution of the World”, Economic Edition,Universal Law Publication Co. Pvt. Ltd., Allahabad, 2002.
- Rastogi, Anirudh.,“Cyber Law-Law of Information Technology and Internet”,1st Edition, Lexis Nexis Publication, Nagpur, 2014.
- Ratanlal, and Dhirajlal., “The Law of Tort”, 26thEdition, Lexis Nexis,Nagpur, 2010.
- Reddy, O. Chinnappa.,“The Court and the Constitution of India: Summits andShallows”, 6thImpression,Oxford University Press, New Delhi, 2013.
- Sathe, S.P., “Right to Information”, LexisNexis, Nagpur, 2006.
- Seervai, H.M., “Constitutional Law of India” 4th Edition Universal Law Publishing, Lexis Nexis, Nagpur, 2015.
- Sharma, S.K., “Privacy Law - A Comparative Study”, Atlantic Publishers and Distributors, New Delhi, 1994.
- Shills, Edward., “Privacy - Its Constitution and Vicissitudes”, 31 Law and Contemporary Problems, (No. 2 Spring), North Carolina,1966.
- Shukla, V.N., “The Constitution of India”, 13th Edition, Eastern Book Company, Lucknow,2017.
- Singh, Avatar., “Principles of the Law of Evidence”, 17thEdition, Central LawPublications, Allahabad, 2009.
- Solove, Daniel J. & Schwartz, Paul M., “Privacy, Information and Technology”, 3rdEdition, Wolters Kluwer Law & Business Publication, New York, 2011.
- Staples. William G., "Encyclopedia of Privacy”, Vol. 1& 2, GreenwoodPress, California, 2007.
- Taneja, Rishika & Kumar, Sidhant.,“Privacy Law-Principles, injunctions and compensation”, 1st Edition, Eastern Book Company, Lucknow, 2014.
- Toulson, R.G. & Phipps, C. M., “Confidentiality”, 2ndEdition, Sweet & Maxwell Ltd. Publication, London, 2006.
- Usha, G., “Cyber Privacy and Security” 1st edition, Icfai University Press, Hyderabad, 2008.

- Vij, Krishan, "Forensic Medicine and Toxicology", 4th Edition, Elsevier,Chennai, 2008.
- Wadehra, B.L., "Law Relating to Intellectual Property", 5th Edition, UniversalLaw Publishing, New Delhi, 2016.
- Yadav, Abhe, Singh., "Right to Information Act, 2005, Analysis", 2ndEdition,Central Law Publications, Allahabad, 2009.

Articles of Indian Journals: -

- Adithan, Dr.Vany., Right to Privacy under Article 21-B, Madras Law Journal,Vol. II, 2003.
- Ahmad, Mohammed., Muslim Law and Reforms: Protection of Privacy in Islam, Civil and Military Law Journal, Vol. 36, 2000.
- Awasthi, Saurabh., Privacy Laws in India: Big Brother is Watching You, Company Law Journal, Vol. 3, 2002.
- Bajwa, Dilbir Kaur., Right to Privacy – its Origin & Ramifications, Civil & Military Law Journal, Vol. 26, 1990.
- Balu, N., State of Maharashtra and Another v. Madhukar Narayan Mardikar and the Right to Privacy, All India Reporter, Vol. 79, 1992.
- Bhandari, Dr. M. K., Right to Privacy Versus Freedom of Press: A Comparative Conspectus of Legal Position in U.S.A., U.K. and India, The Indian Journal of Legal Studies, Vol. XI, 1991.
- Bharuka, Devashish., Piercing the Privacy Veil: A renewed threat, Supreme Court Cases, Vol.1, 2003.
- Deshta, Dr. Sunil. & Deshta, Kiran., Right to Privacy: An Extension ofPersonal Liberty, M.D.U. Law Journal, Vol. X (1), 2005.
- Divan, Madhavi., Right to Privacy in the Age of Information and Communication, Supreme Court Cases, Vol. 4, 2002.
- Goswami, Dhrismitha., "Right to Privacy": In the Perspective of the Information Technology Act, 2000, Gauhati Law Times, Vol. II, 2005.

- Gupta, Shriniwas. & Misra, Dr. Preeti., Right to Privacy – An Analysis of Developmental Process in India, America and Europe, Central India Law Quarterly, Vol.18, 2005.
- Gupta, Shriniwas., Right to Privacy is an Aspect of Human Dignity, Lawyer, Vol. 17, 1985.
- Iyer, Justice V. R. Krishna., Privacy is Human Right, Press Council of India Review, Vol.11, 1990.
- Jain, R. B., The Right to Privacy and Freedom of Information: The Search for a Balance, Indian Journal of Public Administration, Vol.25 (4), 1979.
- Jathin E. J., Human Genome Project: Emerging Challenges of Right to Privacy vis-à-vis Insurer's Right to Know, Cochin University Law Review, Vol. XXXI, 2007.
- Jayashree, L., Right to Privacy of a Woman under Criminal Law, CriminalLaw Journal, Vol.109, 2003.
- Jha, Nemika., Legitimacy of the Right to Privacy as a Fundamental Right – AComparative Study of India and America, All India Reporter, Vol. 88, 2001.
- Joshi, K.C., Right to Privacy: An Extension of Personal Liberty, KurukshetraLaw Journal, Vol. 4, 1978.
- Lal, Prof. S. S., Human Rights and Right to Privacy: In Historical and PresentPerspectives, Journal of the Legal Studies, Vol. XXXVII, 2006-07.
- Lekshmi, G.R., Electronic Surveillance – A Tool for Invasion of Privacy, TheAcademy Law Review, Vol.32:1&2, 2008.
- Noorani, A. G., Right to Privacy, Economic and Political Weekly, Vol.40 (9),2005.
- Noorani, A. G., Privacy vs. Public Interest, Press Council of India Review,Vol.22, 2001.
- Pal Chandra., Right to Privacy - Emerging As a Constitutional Right, Civiland Military Law Journal, (1982).
- Parikh, S. N., Right to Privacy, Civil and Military Law Journal, Vol. 20,1984.

- Pati, Suvendu Kumar., Right to Privacy: Whether Fundamental? Indian Bar Review, Vol. 27, 2000.
- Patnaik, Partha Sarathi.,HIV/AIDS Victim's Right to Privacy, Cuttack Law Times, Vol.88, 1999.
- Pattnaik, Dr. N. C. and Nanda, Dr.Sukanta K., Legal Aspects of Pre-Natal Diagnostic Technique, Central India Law Quarterly, Vol. 18, 2005.
- Pillai, Nirupama. and Ramnath, Kalyani., Trumping Public Interest: Should Violation of Privacy be a Tort?, Cochin University Law Review, Vol. XXX, 2006.
- Prasad, Anirudh., New Dimensions of the Right of Privacy under the Indian Constitution, Journal of Constitutional & Parliamentary Studies, Vol. 4, 1980.
- Qadri, S. M. Afzal., Women and Law relating to Sex Determination Test: With Special Reference to J & K State, Kashmir University Law Review, Vol. XIV.
- Raha, N. K., Right to Privacy under Indian Law, All India Reporter, Vol. 88,2001.
- Reddy, Chidananda., Piety of Privacy after Death, Lawyers Collective, Vol.6,1991.
- Reddy, Dr. S. Srinivas., Right to Privacy of Parties in Matrimonial Disputes –An Analysis, Andhra Law Times, Vol.1, 2009.
- Revathi, R., Pervasive Technology, Invasive Privacy and Lucrative Piracy –A Critique, Journal of the Indian Law Institute, Vol.51(3), 2009.
- Sivakumar, S., Right to Privacy, The Academy Law Review, Vol.18, 1994.
- Sorabjee, Soli J., Privacy and Defamation: SC Defines Parameters, PressCouncil of India Review, Vol. 16, 1995.
- Tageldin, Medani Abdel Rahman., Right to Privacy and Abortion: A Comparative Study of Islamic and Western Jurisprudence, Aligarh Law Journal, Vol. XII, 1997.
- Upadhyay, M. L. and Jayaswal, Prashant., Constitutional Control of Right to Privacy, Central India Law Quarterly, Vol. 2, 1989.

Articles of Foreign Journals: -

- Bamberger, Kenneth A. and Mulligan, Deirdre K., Privacy on the Books and on the Ground, Stanford Law Review, Vol.63 (2), 2011.
- Bignami, Francesca., Case for Tolerant Constitutional Patriotism: The Right to Privacy before the European Courts, Cornell International Law Journal, Vol.41 (2), 2008.
- Chemerinsky, Erwin., Rediscovering Brandeis's Right to Privacy, Brandeis Law Journal, Vol.45 (4), 2007.
- Cohen William and David J. Danelski., Constitutional Law: Civil Liberty and Individual Rights, New York Foundation Press, IV Edition, 1997.
- Harris, Donald., A Matter of Privacy: Managing Personal Data in Company Computers, Personnel, Vol.64 (2), 1987.
- Kaplan, Benjamin J., Fictions of Privacy: House Chapels and the Spatial Accommodation of Religious Dissent in Early Modern Europe, American Historical Review, Vol.107 (4), 2002.
- Kenyon, T. Andrew., New Dimensions in Privacy Law, Cambridge University Press, 2007.
- Kim, Mun-Cho., Surveillance Technology, Privacy and Social Control: With Reference to the Case of the Electronic National Identification Card in South Korea, International Sociology, Vol.19 (2), 2004.
- Levinson, Sanford., Public Lives and the Limits of Privacy, PS: Political Science and Politics, Vol.21 (2), 1988.
- Libbin, Anne E. Mendelsohn, Susan R. and Duffy, Dennis P., The Right to Privacy at the Workplace: Employee Medical and Honesty Testing, Personnel, Vol.65 (11), 1988.
- Loring, Tracie B., Analysis of the Informational Privacy Protection afforded by the European Union and the United States, Texas International Law Journal, Vol.37 (2), 2002.

- Margulis, Stephen T., On the Status and Contribution of Westin's and Altman's Theories of Privacy, Journal of Social Issues, Vol.59 (2), 2003.
- McGhee, Derek., Beyond Toleration: Privacy, Citizenship and Sexual Minorities in England and Wales, British Journal of Sociology, Vol.55 (3), 2004.
- Mendelson, Susan R. & Morrison, Kathryn K., The Right to Privacy in the Workplace: Testing Applicants for Alcohol and Drug Abuse, Personnel, Vol.65(8), 1988.
- Regan, Priscilla M., Privacy, Government, Information and Technology, Public Administration Review, Vol.46 (6), 1986.
- Smith, H. Jeff., Information Privacy and Marketing: What the US should (andshouldn't) learn from Europe, California Management Review, Vol.43 (2), 2001.
- Warren, Samuel D. and Brandeis, Louis D., The Right to Privacy, Harvard Law Review, Vol. IV (5),1890.

Reports*:* -

- Databanks in a Free Society: Computers, Record-Keeping and Privacy – A Report by Alan F. Westin, Project Director and Michael A. Baker, Assistant Project Director, Quadrangle Books Publication, New York, 1972.
- Human Rights and Scientific and Technological Development: Studies on theAffirmative use of Science and Technology for the furtherance of Human Rights – A Report of a Special Project commissioned by the United Nations University, following a Reference to the University by the United Nations Human Rights Commission, Edited by C. G. Weeramantry.
- Privacy and Personal Information, Australian Law Reform Commission, 1980
- Privacy and the Law: A Report of the International Commission of Jurists, Great Britain, Sweet & Maxwell Publication, London, 1970.
- Report of the Committee on Privacy – London: Her Majesty's Stationary Office, United Kingdom, 1972.

- The Computer and Invasion of Privacy: Hearings, 89th Congress, 2nd Session

  – A Report of the Special Sub-Committee on Invasion of Privacy, Committee on Government Operations, U.S. Congress House, U.S. Government Publication, Washington, 1966.
- The Final Report of the Royal Commission on the Press in U.K., 1977.
- The Younger Committee Report on Privacy in U.K., 1972.

Journals*:* -

- All India Reporter.
- American Historical Review.
- Andhra Law Times.
- Brandeis Law Journal.
- British Journal of Sociology.
- California Management Review.
- Civil and Military Law Journal.
- Cornell International Law Journal.
- Criminal Law Journal.
- Dr. Ram Manohar Lohiya National Law University.
- Harvard Law Review.
- Indian Bar Review.
- Indiana Law Journal.
- International Journal of Public Administration.
- International Sociology.
- Journal of Social Issues.
- Journal of The Indian Law Institute.
- Organizational Dynamics.
- Parliamentary Affairs.
- Personnel.
- PS : Political Science and Politics.
- Public Administration Review.

- Punjabi University Law Journal.
- Stanford Law Review.
- Supreme Court Cases.
- Supreme Court Journal.
- Texas International Law Journal.
- The Academy Law Review.
- The Gauhati Law Times.
- The Karnataka Law Journal.
- The Lawyers Collective.
- The Madras Law Journal.
- The Press Council of India Review.
- The Yale Law Journal.

Web Pages: -

- www.jstor.org
- www.legalindia.com
- www.scconline.com
- www.prsindia.org
- www.slideshare.net
- www.legalserviceindia.com
- www.livelaw.in
- www.lexisnexis.com
- www.westlawindia.com
- www.manupatrafast.com
- www.worldcat.org
- htpp://www.ftc.gov/bcp/conline/pubs/buspubs/glbshort.html
- htpp://www.hhs.gov/news/facts/privacy.html
- htpp://www.hhs.gov/ocr/hipaa/privrulepd.pdf
- http.//www.legal service India.com/article/1384-legalize-Abortion-in-India
- http://canada.justice.gc.ca/en/ps/atip/provte.html.

- http://courtnic.nic.in/supreme court/temp/dc%201798509p.txt
- http://downloads.bbc.co.uk/guidelines/editorialguidelin es/Legacy- Guidelines/2000-producers-guidelines.pdf,
- http://dx.doi.org/10.2139/ssrn.1807733
- http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp39 en.htm
- http://indiatoday.intoday.in/story/data-collected-for-supreme-court-centre/1/350993.html
- http://lawmin.nic.in/ncnvc/finalreport/vlch3.html
- http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2350631
- http://www.canada.justice.qc.ca/stable/EN/laws/chap/p/p_21.html.
- http://www.cas.okstate.edu/jb/faculty/senat/jb 3163 /privacytorts.html
- http://www.cia.gov/library/publications/the-world-factbook/geos/in.html
- http://www.datenschutz-berlin.de/gesetze/bdsg/bdsgeng.htm.
- http://www.ecom.jp/qecom/ecom_e/index.html.
- http://www.ftc.gov/opa/2001/10/privacyagenda.htm,
- http://www.ftc.gov/os/2002/04/coppasurvey.pdf
- http://www.jus.uio.no/iri/rettsinfo/lib/papers/dp_norway.html.
- http://www.ntt.co.jp/japan/constitution/englishconstitution.html.
- http://www.nyulawglobal.org/globalex/india.htm
- http://www.nyulawglobal.org/globalex/india.htm
- http://www.nyulawglobal.org/globalex/india.htm
- http://www.sarai.net/publications/readers/07-frontiers/100-110_lawrence.pdf.
- http://www.ssrn.com/abstract=2133915.
- http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paip-pefr_e.asp.
- https://dictionary.cambridge.org/dictionary/english/paparazzi
- https://globalfreedomofexpression.columbia.edu/cases/central-public- information-officer-supreme-court-of-india-v-subhash-chandra-agarwal/.
- https://thewire.in/law/jamaica-supreme-court-aadhaar-justice-chandrachud.

- https://uidai.gov.in/legal-framework/aadhaar-act.html.
- https://www.britannica.com/event/bowers-v-hardwick
- https://www.caselaw.findlaw.com/us-supreme-court/431/494.
- https://www.supremecourt.gov.in/supremecourt/2012/35071/35071_2012_Order_15-Dec-2017.
- https://www.supremecourtofindia.nic.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf
- www.academia.edu/237240/TheRight_to_Privacy_An_Emerging_Right_in_Chinese_Law.pdf
- www.cis-india.org/internet-governance/blog/leaked-privacy-bill-20142011.html
- www.cyberlawcentre.org/appcc/announce.htm
- www.ejbss.com/Data/Sites/1/octoberissue/ejbss-12-1164therighttoprivacy.pdf
- www.ejcl.or/121/art 121-20.pdf
- www.ejcl.org/131-2.pdf
- www.epic.org/ privacy/medical/medical-privacy-399.pdf.
- www.epic.org/privacy/1974act.html
- www.gilc.nl/privacy/survey/surveyak.html
- www.indiankanoon.org/doc/1987982.html
- www.judis.nic.in/supremecourtofindia.pdf
- www.lawtechnologytoday.org
- www.legalparley.com/rti-and-right–to–privacy.html
- www.loenel.ch/docs/history-of-sa-law-en.pdf
- www.presscouncil.nic.in/NORMS2010.pdf
- www.shodhganga.inflibnet.ac.in/bitstream
- www.supreme.justia.com/cases/federal/us/277/438/case.html
- www.supremecourtofindia.nic.in/supremecourt
- www.victoria.ac.nz/law/research/publications/vuwlr/prev-issues/pdf/vol-36-2005/issue-3/jingchum.pdf