

# **Legal and Regulatory Issues of Privacy and Data Protection in e-Commerce: An Analytical Study**

A Thesis Submitted

To

**Sikkim University**



In Partial Fulfilment of the Requirement for the  
**Degree of Doctor of Philosophy**

By

**Sambhavna Rai**

Department of Law

School of Social Sciences

May 2020

Date: 14.08.2020

## DECLARATION

I, **SAMBHAVNA RAI**, hereby declare that the research work hereby embodied in the thesis titled **“Legal and Regulatory Issues of Privacy and Data Protection in e-Commerce-An Analytical Study”** submitted to the Sikkim University in partial fulfillment of the requirement for the **Degree of Doctor of Philosophy** is my original work. This thesis has not been submitted for any other degree of this University or any other University.



**SAMBHAVNA RAI**

Ph.D. Registration No.: 16/Ph.D/LAW/01

Registration Date: 22.05.2017

Department of Law

School of Social Sciences

6 माइल, सामदुर, तादोंग -737102  
गंगटोक, सिक्किम, भारत  
फोन-03592-251212, 251415, 251656  
टेलीफैक्स -251067  
वेबसाइट - [www.cus.ac.in](http://www.cus.ac.in)



## सिक्किम विश्वविद्यालय SIKKIM UNIVERSITY

6<sup>th</sup> Mile, Samdur, Tadong -737102  
Gangtok, Sikkim, India  
Ph. 03592-251212, 251415, 251656  
Telefax: 251067  
Website: [www.cus.ac.in](http://www.cus.ac.in)

(भारत के संसद के अधिनियम द्वारा वर्ष 2007 में स्थापित और नैक (एनएएसी) द्वारा वर्ष 2015 में प्रत्यायित केंद्रीय विश्वविद्यालय)  
(A central university established by an Act of Parliament of India in 2007 and accredited by NAAC in 2015)

Date: 14-08-2020

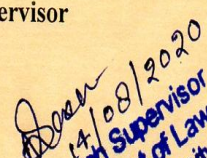
### CERTIFICATE

This is to certify that Thesis Titled “Legal and Regulatory Issues of Privacy and Data Protection in e-Commerce: An Analytical Study” submitted to the Sikkim University for the partial fulfillment of the degree of Doctor of Philosophy in the Department of Law, embodies the result of bonafide research work carried out by SAMBHAVNA RAI under my guidance and supervision. No part of the dissertation has been submitted for any other Degree, Diploma, Association and fellowship.

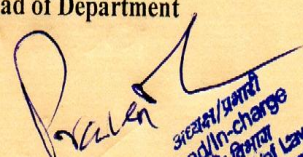
All the assistance and help received during the course of investigation have been duly acknowledge by him.

We recommend that this thesis be placed before the examiner for evaluation.

Supervisor

  
14/08/2020  
Research Supervisor  
Department of Law  
Sikkim University  
Dr. Nidhi Saxena  
Assistant Professor  
Department of Law  
School of Social Sciences  
Sikkim University

Head of Department

  
अध्यक्ष/प्रभारी  
Head/In-charge  
विधि विभाग  
Department of Law  
सिक्किम विश्वविद्यालय  
Sikkim University  
Dr. Pravin Mishra  
Associate Professor  
Department of Law  
School of Social Sciences  
Sikkim University



6 माइल, सामदुर, तादोंग -737102  
गंगटोक, सिक्किम, भारत  
फोन-03592-251212, 251415, 251656  
टेलीफैक्स -251067  
वेबसाइट - [www.cus.ac.in](http://www.cus.ac.in)



6<sup>th</sup> Mile, Samdur, Tadong -737102  
Gangtok, Sikkim, India  
Ph. 03592-251212, 251415, 251656  
Telefax: 251067  
Website: [www.cus.ac.in](http://www.cus.ac.in)

## सिक्किम विश्वविद्यालय SIKKIM UNIVERSITY

(भारत के संसद के अधिनियम द्वारा वर्ष 2007 में स्थापित और नैक (एनएएसी) द्वारा वर्ष 2015 में प्रत्यायित केंद्रीय विश्वविद्यालय)  
(A central university established by an Act of Parliament of India in 2007 and accredited by NAAC in 2015)

Date: 14.08.2020

### PLAGIARISM CHECK CERTIFICATE

This is to certify that plagiarism check has been carried out for the following Ph.D. thesis with the help of **URKUND SOFTWARE** and the result is 8% tolerance rate, which is within the permissible limit (below 10%) as per the norm of Sikkim University.

#### “LEGAL AND REGULATORY ISSUES OF PRIVACY AND DATA PROTECTION IN E-COMMERCE: AN ANALYTICAL STUDY”

Submitted by (*Sambhavna Rai*) under the supervision of (*Dr. Nidhi Saxena*,  
*Assistant Professor, Department of Law, School of Social Sciences, Sikkim  
University*) Gangtok, Pin 737101, India.

*Sambhavna Rai* 14/08/2020

Signature of the Scholar  
(SAMBHAVNA RAI)

*Nidhi Saxena* 14/08/2020  
Countersigned by the Supervisor  
Research Supervisor  
Department of Law  
Sikkim University

*Achanda* 14/08/2020

Vetted by Librarian  
पुस्तकालयाध्यक्ष  
Librarian

श्रीव पुस्तकालय Central Library  
सिक्किम विश्वविद्यालय  
Sikkim University

## CONTENTS

	<b>Page(s)</b>
<i>Acknowledgement</i>	<b>i-iii</b>
<i>List of Cases</i>	<b>iv-viii</b>
<i>List of Abbreviations</i>	<b>ix-xii</b>
<i>Executive Summary</i>	<b>xiii-xv</b>

### **CHAPTER ONE: INTRODUCTION**

1.1	Introduction	1
1.2	Privacy	7
1.3	Data	11
1.4	E-Commerce	11
1.5	Choice of Forum	13
1.6	Choice of Jurisdiction	13
1.7	Statement of Problem	14
1.8	Literature Review	20
1.9	Rationale & Scope of the Study	26
1.10	Research Objectives	26
1.11	Research Questions	27
1.12	Hypothesis	27
1.13	Research Methodology	27

### **CHAPTER TWO: LEGAL AND TECHNO-LEGAL ISSUES IN PRIVACY AND DATA PROTECTION IN e-COMMERCE**

2.1.	Introduction	29
2.2.	Origin and Development of Privacy	32
2.3.	The legal issues of privacy and data protection in e-Commerce	34
2.3.1.	Privacy under Indian Laws	34
2.3.1.1.	Constitutional Law of India	34
2.3.1.1.1.	Legal issues in defining privacy	39
2.3.1.1.1.i.	Territorial Privacy	43
2.3.1.1.1.ii.	Online Privacy	44
2.3.1.1.1.iii.	Data privacy or Information Privacy	44
2.3.1.2.	Indian Laws on Privacy and Data Protection	44
2.3.1.2.1.	The Information Technology Act, 2000 (Act 21 of 2000)	45
2.3.1.2.2.	The Information Technology (Amendment) Act, 2008	47
2.3.1.2.3.	The Indian Contract Act, 1872	48
2.3.1.2.4.	The Securities and Exchange Board of India (SEBI) Act, 1992	50
2.3.1.2.5.	The Consumer Protection Act, (COPRA) 1986	52



### **CHAPTER THREE: LEGAL FRAMEWORK FOR PRIVACY & DATA PROTECTION IN e-COMMERCE AND INTERNATIONAL DOCUMENTS**

3.1. Introduction	92
3.2. Legal Framework for Privacy –Indian Scenario	94
3.2. i. Privacy under the Constitution of India	94
3.2. ii. Jurisprudential aspect of privacy	98
3.2.iii. Privacy under law of Tort	99
3.2.iv. Privacy under the Information Technology Act, 2000	100
3.2.v. Privacy under the Information Technology (Amendment) Act, 2008	103
3.2. vi. Privacy under the Consumer Protection Act, 1986	105
3.2.vii. Privacy under Indian Penal Code, 1860 and Indian Evidence Act, 1872	105
3.2.viii. Online Privacy under Securities Exchange Board of India Guidelines	106
3.2.ix. Privacy under R.B.I. Guidelines	106
3.3. Legal Framework for Data Protection: Indian Scenario	107
3.3.i. Data privacy under Information Technology Act, 2000 (Act No. 21 of2000)	107
3.3.ii. Data privacy under Information Technology (Amendment) Act, 2008	108
3.3.iii. White Paper on Data Protection (November 27, 2017)	109
3. 4. Privacy and Data Protection: International Scenario	111
3.4.i. World Trade Organisation, (W.T.O.)	112
3.4.ii. Organization for Economic Cooperation and Development (OECD)	114
3.4.iii. Asia-Pacific Economic Cooperation (APEC)	120
3.4.iv. World Intellectual Property Organization (WIPO)	121
3.4.v. Trade Related Intellectual Property Rights (TRIPS)	122
3.4.vi. European Convention on Human Rights (ECHR)	123
3.4.vii. International Criminal Police Organization (INTERPOL)	125
3.4.viii. G7 & G8 Group	126
3.4.ix. International Chamber of Commerce (ICC)	127
3.5. Conclusion	128

### **CHAPTER FOUR: REGULATORY ISSUES INVOLVED IN PROTECTION OF PRIVACY AND DATA PRIVACY IN e-COMMERCE**

4.1. Introduction	129
4.2. Regulatory issues under Domestic Law	132
4.2.i. Code of Civil Procedure, 1908 (C.P.C.)	132
4.2.ii. Indian Penal Code, 1860 (I.P.C.)	134

4.2.iii.	Indian Contract Act, 1872	135
4.2.iv.	Information Technology (Amendment) Act, 2008	137
4.2.v.	Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011	138
4.2.vi.	Personal Data (Protection) Bill, 2013	139
4.2.vii.	Information Technology (Intermediaries Guidelines) Rules, 2011	140
4.3.	Other Regulatory issues at Domestic Level	143
4.3.1.	Issues of security in e-Commerce	143
4.3.2.	Issues of liability of intermediaries in e-Commerce transaction	143
4.3.3.	Issues of choice of law in e-Commerce	144
4.3.4.	Issues of choice of forum in e-Commerce	145
4.3.5.	Issues of choice of jurisdiction in e-Commerce	146
4.4.	Regulatory Issues at International Level	155
4.4.1.	Choice of law and Jurisdictional issue in European Union and United States	155
4.4.1.i.	Issues of choice of law in European Union	156
4.4.1.ii.	Issues of choice of Jurisdiction in European Union	158
4.4.1.iii.	Brussels Regulation	158
4.4.1.iv.	Issues of choice of Law in United States	158
4.4.1.v.	Issues of choice of Jurisdiction in Unites States	159
4.5.	Principles and Guideline for privacy and data under International Organizations and Documents	161
4.5.1.	The OECD Principles/ Guidelines on the Protection of Privacy and Transborder flows of Personal Information	161
4.5.2.	The Hague Convention on issues of conflict of law	162
4.5.3.	Trade Related Intellectual Property Rights (TRIPS) on Data Protection	162
4.6.	Conclusion	165

## **CHAPTER FIVE: COMPARATIVE STUDY OF PRIVACY AND DATA PROTECTION LAWS IN e-COMMERCE**

5.1.	Introduction	167
5.2.	Privacy and Data Protection laws in United Kingdom (U.K.)	168
5.2.1.	U.K.'s Younger Committee Report on Privacy, 1973	170
5.2.2.	Data Protection Directive (95/46/EC)	171
5.2.3.	Data Protection Act of 1984	173
5.2.4.	Data Protection Act of 1998	173
5.2.5.	Data Protection Act, 2018	174
5.3.	Privacy and Data Protection laws in European Union	174
5.3.1.	Data Protection Directive (95/46/EC)	175
5.3.2.	Directive on e-Commerce 2000/31/EC 8 June 2000 (ECD)	176



5.3.3.	European Union’s Data Protection Act of 2018	178
5.3.4.	General Data Protection Regulation, 2018 (GDPR)	179
5.4.	Privacy and Data Protection laws in the United States (U.S.)	180
5.4.1.	The Fair Credit Reporting Act (FCRA), 1970	182
5.4.2.	Privacy Act 1974	182
5.4.3.	Family Educational Rights and Privacy Act, 1974 (FERPA)	182
5.4.4.	Cable Communications Policy Act, 1984	183
5.4.5.	Electronic Communications Privacy Act, 1986	183
5.4.6.	Computer Matching and Privacy Act of 1988	184
5.4.7.	The Video Privacy Protection Act (VPPA), 1988	184
5.4.8.	The Telephone Consumer Protection Act (TCPA), 1991	184
5.4.9.	The Driver’s Privacy Protection Act (DPPA), 1994	185
5.4.10.	The Health Information Portability and Accountability Act (HIPPA), 1996	185
5.4.11.	Children’s Online Privacy Protection Act, 1998 (COPPA)	185
5.4.12.	The Gramm Leach Bliley Act (GLBA), 1999	186
5.4.13.	PATRIOT Act, 2011	186
5.5.	Privacy and Data Protection: Indian Scenario	187
5.5.1.	The Constitution of India	188
5.5.2.	The Right to Information Act, 2005	191
5.5.3.	The Information Technology (Amendment) Act, 2008	192
5.5.4.	The Personal Data (protection) Bill 2013	192
5.5.5.	Intellectual Property Rights (I.P.R.s)	193
5.6.	Comparison between Countries	194
5.7.	Conclusion	195

**CHAPTER SIX: CONCLUSION AND SUGGESTIONS** **198-211**

REFERENCES

## **ACKNOWLEDGEMENT**

Date: 14.08.2020

I have always been fascinated by the work of Dr. Nidhi Saxena, Assistant professor, Department of Law, Sikkim University. Her knowledge about our Constitution and Cyber Laws is highly commendable and has left a great impact on all the law students and scholars of our department. It was matter of great joy and blessing to have her as a supervisor for my Ph.D. thesis. I would like to express special gratitude towards my supervisor for her valuable guidance and support in completing my work. For a toddler like me in the research world, her immense support from selection of topic to its completion has been incredible. No words would suffice my deepest sense of gratefulness towards her contribution, love and patience towards me during all these years. My research work is the outcome of her cooperation as well as advices. She has been my mentor and source of inspiration and will continue to be one.

I would like to take this opportunity to express my deepest and sincere gratitude towards Hon'ble Mr. Justice , Arup Kumar Goswami, Chief Justice, High Court of Sikkim for his generosity to provide me the liberty to work on my thesis and also for being kind towards me and allowing me to attend all the necessary seminars and presentations during the office hours. My work would not have been complete without his support and cooperation. I would always remain grateful to him.

The completion of this work would not have been complete without the suggestions and assistance of Dr. Veer Mayank, Assistant Professor, Department of Law, Sikkim University. His helpful research advices and analysis has played a great role in shaping my work. I would always remain grateful towards him.

I would like to acknowledge my deepest gratitude towards Head of Department, Law, Associate Professor Dr. Pravin Mishra and Professor Imtiaz Gulam Ahmed (former H.O.D.) for their support, guidance and advices during my research work. Their suggestions have really helped me during the course of work. I am grateful to Dr. Pramita Gurung, Assistant Professor, ICFAI University, Sikkim for providing me the information regarding publication of articles, writing instructions as well as her research journey. Her support has been truly helpful. I am also grateful to Dr. Denkila Bhutia, Assistant Professor, Department of Law Sikkim University for giving me knowledge about Plagiarism issues and the information regarding how a researcher can avoid plagiarism. Her golden tips have really helped in achieving the goal. I would also like to acknowledge Dr. Sonam Yangchen Bhutia, Assistant Professor, Department of Law Sikkim University, for her concern regarding my research and her valuable advices to complete the work on time.

I am grateful to Hon'ble Vice Chancellor, Professor Avinash Khare and all the former Vice Chancellor's of Sikkim University for the opportunity and facilities provided to the research scholars of our University in completing the research work.

I am grateful to the library staffs of Sikkim University, High Court of Sikkim, National Law School of India University (NLSIU) and North Bengal University (N.B.U.) for the immense support and guidance while I was researching and collecting the necessary materials. Without their guidance the research work would have been really time taking and painful.

I am highly indebted towards the University Grant Commission for providing me with the Scholarship for undertaking this research work. Without their support this research work would have been really difficult.

I would also like to acknowledge the moral support and guidance of my fellow scholar friend, Naina Thatal, Ph.D. Research Scholar, Department of Sociology, Sikkim University for her valuable time and support .Her support has really helped me in times of self doubt. I would also take this opportunity to express my deep sense of gratitude to Mr. Nithil Raika Thapa, Librarian, High Court of Sikkim for providing me with necessary guidance and support during the completion of this research work.

I would also like to extend my thanks to my fellow Ph.D. research scholars, Sikkim University specially Jigme Wangchuk Bhutiafor the constant support and encouragement.I would further extend my thanks to my childhood friend Ms. Primulla Rajani Chamling for the constant support, believe and unconditional love. I would also like to acknowledge my sincere thank to Mrs. Shweta Pakhrin Rai and Advocate Monica Rai, for their moral support and guidance.

Last, but not the least I would like to thank my parents and God for giving me the strength and valuable support throughout this journey. Their conviction on me has been a source of great inspiration in completion of this work.

- **Sambhavna Rai**



## LISTS OF CASES

1. Abdul Wazid vs. Vishwanathan, AIR 1975 Mad.261
2. ADM Jabalpur vs. Shivkant Shukla, (1976) 2 SCC 521
3. ACLU vs. Reno, 521 US 844
4. A.K. Gopalan vs. State of Tamil Nadu, AIR 1950 SC 27
5. Asahi Metal Industries vs. Superior Court 480 U.S. 102 (1987)
6. Bandhua Mukti Morcha vs. Union of India, (1984) 3 SCC 161
7. Banyan Tree Holding (P) Limited vs. A. Murali Krishna Reddy and Ors. ,  
(2009) SCC OnLine Del 3780
8. Bannett Coleman vs. Union of India, AIR 1973 SC 60
9. Binoy Visman vs. Union of India, (2017) 7 SCC 1
10. Board of Education of Independent School District No. 92 of Pottawatomie  
County et al. vs. Earls et al., 2002 SCC OnLine US SC 75: 536 US 822 (2002)
11. Burger King Corp. vs. Rudzewicz 471 U.S. 462 (1985)
12. Calder vs. Jones, 465, U.S. 783 (1984)
13. Casio India Co. Ltd vs. Ashita Tele Systems Pvt. Ltd. 2003 Del.
14. Connecticut Dept. of Public Safety vs. Doe, 538 US 1 (2003)
15. Consim Info. Pvt. Ltd vs. Google India Pvt. Ltd. & Ors., 2013 (54)PTC 578  
(Mad.)
16. Corinthian Pharmaceutical Systems Inc. vs. Lederle Laboratories, 724 F.  
Supp. 605, 1989 U.S. Dist.13058
17. Cybersell, Inc. vs. Cybersell, Inc. (US App LEXIS 33871 1997)
18. Dhannalal vs. Kalawatibai, (2002) 6SCC 16
19. District Registrar and Collector vs. Canara Bank, (2005) 1 SCC 596

20. Doe vs. Chao, 540 US 614(2004)
21. Francis Coralie Mullin vs. UT of Delhi, (1981) 1 SCC 608
22. Gobind vs. State of Madhya Pradesh and Another, (1975) 2 SCC 148
23. Gokal Prasad vs. Radho, (1888) ILR 10 All 358
24. Golak Nath vs. State of Punjab, (1976) 2 SCR 762
25. Gonzaga Univ. vs. Doe, 536 US 273 (2002)
26. Griswold vs. State of Connecticut, 1965 SCC OnLine US SC 124
27. Hakam Singh vs. Gammon (India) Ltd., (1971) 1 SCC 286
28. Hanson vs. Denckla (2L.Ed.2d 1283 1958)
29. Hiibel vs. Sixth Judicial District Court of Nevada Humboldt County et al.,  
2004 SCC OnLine US SC 55: 542 US 177 (2004)
30. House vs. Pith (1956)
31. Illinois vs. Caballes, 543 US 405 (2005)
32. Indira Nehru Gandhi vs. Raj Narain, 1975 Supp SC 1
33. India TV vs. India Broadcast Live, 2007 Delhi HC
34. Indian Express Newspaper (Bombay) vs. Union of India, (1985) 1 SCC 641
35. Inflow Technologies Pvt. Ltd vs. Yahoo India Pvt. Ltd, 2014 SCC OnLine  
Bom 121: (2014) 4 Bom CR690
36. International Shoe Co. vs. Washington 326 U.S. 340 (1945)
37. IPRS vs. Sanjay Dalia, 2008 Delhi HC
38. I.R. Coelho vs. State of Tamil Nadu, (2007) 2 SCC 1
39. Jeeja Ghosh vs. Union of India, (2016) 7 SCC 761
40. Kesavananda Bharati vs. State of Kerala, (1973) 4 SCC 225
41. Kharak Singh vs. State of Uttar Pradesh, AIR 1963 SC 1295: (1964) 1 SCR

42. Khedat Mazdoor Chetna Sangath vs. State of M.P., (1994) 6 SCC 260
43. Kottabomman Transport Corporation Limited vs. State of Travancore and others, AIR 1992 Ker.351
44. K.P.M. Builders Private Limited vs. National Highways Authority of India and Another, (2015) 15 SCC 394
45. K.S. Puttaswami vs. Union of India, (2017) 10 SCC 1
46. Kyllo vs. United States, 2001 SCC OnLine US SC 61:533 US 27 (2011)
47. Lalji Raja and Sons vs. Firm Hansraj Nathuram, AIR 1971 SC 974
48. LTU vs. Euro Control (1 CMLR 293 1997)
49. Maneka Gandhi vs. Union of India , (1978) 1 SCC 258
50. Metaspinner Media GmbH vs. Google Deutschland, No. 312 O 887/02
51. Minerva Mills Ltd. vs. Union of India, (1980) 3 SCC 625
52. M. Nagaraj vs. Union of India, (2006) 8 SCC 212
53. M.P. Sharma vs. Satish Chandra (1954) 1SCR 1077
54. Maharashtra University of Health Sciences vs. Satchikitsa Prasarak Mandal, (2013) 3 SCC 786
55. Mehmood Nayyar Azam vs. State of Chattisgarh, (2012) 8 SCC 1
56. Modi Entertainment Network and Another vs. W.S.G. Cricket PTE. Ltd, (2003) 4 SCC 341
57. National Archives & Records Administration vs. Favish, 541 US 157 (2004)
58. Narhari vs. Pannclal, AIR 1977 SC 164
59. National Legal Services Authority vs. Union of India, (2014) 5SCC 438
60. NAZ Foundation vs. Government of NCT, (2014) 1 SCC 1
61. Nemetschek AG vs. Google, LG Munich, No. 33 O 21461/03
62. Netherlands State vs. Ruffer (3 CMLR 2931981)

63. Olga Tellis vs. Bombay Municipal Corpn, (1985) 3 SCC 545
64. Onkar Lal Bajaj vs. Union of India, (2003) 2 SCC 673
65. Olmstead vs. Unites States (1928)
66. Prajwala Letter Dated 18-02-2015 Videos of Sexual Violence and Recommendation, in RE, (2018) 17 SCC 79
67. P.D. Shamdasani vs. Central Bank of India Ltd. , AIR 1952 SC 59: 1952 SCR 597
68. Prem Shankar Shukla vs. Delhi Admn., (1980) 3 SCC 526
69. PUCL vs. Union of India, (1997) 1 SCC 301 [Equivalent Citations: (2019) 15 SCC 748]
70. Ram Jethamalani & Ors. vs. Union of India, (2011) 8SCC1
71. R.C. Cooper vs. Union of India, AIR 1950 SC 27
72. Reed Elsevier, Inc. vs. Innovator Corpn., No. C-3-99-141(March 10, 2000)
73. Registrar and Collector, Hyderabad and Anr. vs. Canara Bank Etc., AIR 2004 SC 935
74. Religious Tech. Ltr. vs. F.A.C.T. Net, Inc., 901 F. Supp.1519 (D. Colo. 1995)
75. Religious Tech. Ltr. vs. Lerma, 897 F. Supp. 260 (E.D. Va.1995)
76. Reno vs. Condon, 2000 SCC OnLine US SC 4: 528 US 141 (2000)
77. R. Rajagopal vs. State of Tamil Nadu, (1994) 6SCC 623 [Auto Shanker Case]
78. Rustom Cavasjee Cooper, (1970) 1 SCC 248
79. Shabnam vs. Union of India, (2015) 6 SCC 702
80. Sharda vs. Dharampal, AIR 2003 SC 3450
81. Shakankarlal Agarrwalla vs. State Bank of India, AIR 1987 Cal 29
82. Shreya Singhal vs. Union of India, (2015) 5SCC 1
83. State of Karnataka vs. Krishnapa, AIR 2000 SC 1470



84. State vs. N.M.T. Joy Immaculate, AIR 2004 SC 2282
85. Supreme Court of India vs. Subhash Chandra Agarwal, 2009 SCC OnLine Del 2714: (2019) 162 DLT 135
86. Thornton vs. United States, 271 US 414 (1926)
87. Union of India vs. Bhanudas Krishna Gawde, (1977) 1 SCC 834
88. Unni Krishnan, J.P. vs. State of A.P., (1993) 1SCC 645
89. United States vs. Flores-Montano, 541 US 149 (2004)
90. Vishaka vs. State of Rajasthan, AIR 1997 SC 3011
91. Watchtower Bible & Tract Society of New York, Inc., et al. vs. Village of Stratton et.al, 2002 SCC OnLine US SC 55: 526 US 150 (2002)
92. World Wrestling Entertainment vs. M/S Reshma Collection & Ors., FAO (OS) No. 506 of 2013
93. X vs. Hospital Z, AIR 1999 SC 495
94. Yahoo, 2001 Us Dist. LEXIS 18378 (N.D. Cal. 2001) & 145 F. Supp.2d 1168 (N.D. Cal. 2001)

## ABBREVIATIONS

AIR	: All India Report
ALL ER	: All England Law Report
APEC	: Asia Pacific Economic Co-operation
Art. (s)	: Article (s)
ATM	: Automatic Teller Machine
B2C	: Business to Consumer
C.A.T.	: Cyber Appellate Tribunal
C.C.T.V.	: Closed-Circuit Television
COPPA	: Children’s Online Privacy Protection Act
COPRA	: Consumer Protection Act
C.P.C.	: Civil Procedure Code
Cr.L.J.	: Criminal Law Journal
Cr.P.C.	: Criminal Procedure Code
DNS	: Domain Name System
DPA	: Data Protection Act
DPPA	: The Driver’s Privacy Protection Act
DPR	: Data Protection Registrar
D.O.S.	: Denial of Service
E-Commerce	: Electronic Commerce
EC	: European Commission
E-Contract	: Electronic Contract
E-Com	: Electronic Commerce

ECD	: E-Commerce Directives
ECHR	: European Convention on Human Rights
ECMS	: Electronic Copyright Management Systems
EDA	: Exploratory Data Analysis
EFTA	: European Free Trade Association
E-Mail	: Electronic Mail
E-Media	: Electronic Media
E-Transaction	: Electronic Transaction
E-Users	: Electronic Users
EU	: European Union
FCRA	: The Fair Credit Reporting Act
FERPA	: Family Educational Rights and Privacy Act
G	: Group
GATT	: General Agreement on Tariffs and Trade
GDPR	: General Data Protection Regulation
GIFs	: Graphics Interchange Format
GLBA	: The Gramm Leach Bliley Act
HIPPA	: The Health Information Portability and Accountability Act
HTTP	: Hypertext Transfer Protocol
ICA	: Indian Contract Act
ICC	: International Chamber of Commerce
ICCPR	: International Covenant on Civil and Political Rights
ICT	: Information and Communication Technology

ID	: Identifier Number
ILI	: Indian Law Institute
INTERPOL	: International Criminal Police Organization
IMEI	: International Mobile Equipment Identity
IOT	: Internet of Things
IP	: Intellectual Property
IPR	: Intellectual Property Rights
IPS	: Intrusion Prevention
IDS	: Intrusion Detection
ISPs	: Internet Server Provider
I.T.	: Information Technology
I.T.A.	: Information Technology Act
I.T.A.A.	: Information Technology (Amended) Act
L.P.G.	: Liquefied Petroleum Gas
MEITY	: Ministry of Electronics and Information Technology
OECD	: Organisation for Economic Co-operation and Development
OSNs	: Online Social Networks
P.M.	: Prime Minister
PPDM	: Privacy-Preserving Data Mining
P3P	: Platform for Privacy Preferences
R.B.I.	: Reserve Bank of India
RTI	: Right to Information
RFID	: Radio-Frequency Identification



SC	: Supreme Court
SCC	: Supreme Court Cases
SEBI	: The Securities and Exchange Board of India
SIM	: Subscriber Identification Module / Subscriber Identity Module
SSL	: Secure Data Layer
TCPA	: The Telephone Consumer Protection Act
TLI	: Tulane Law Institute
TRAI	: Telecom Regulatory Authority of India
TRIPS	: Trade Related Intellectual Property Rights
UDHR	: Universal Declaration of Human Rights
UID	: Unique Identity Number
UIDAI	: Unique Identification Authority of India
UNCITRAL	: United Nations Commissions on International Trade Law
URL	: Uniform Resource Locator
U/S	: Under Section
U.S.A.	: United States of America
U.S.	: United States
U.K.	: United Kingdom
VPPA	: The Video Privacy Protection Act
WIPO	: World Intellectual Property Organisation
W.T. O.	: World Trade Organisation
W3C	: World Wide Web Consortium
WWW	: World Wide Web

## Executive Summary

This work is divided into six chapters wherein the first chapter is 'Introductory'. This introductory part of my thesis which is titled as 'Legal and Regulatory Issues of privacy and Data Protection in e-Commerce: An Analytical Study', is the preamble of the inclusive thesis. Introduction, Statement of problem, Literature Review, Research Objectives, Research Questions, Hypothesis, Rationale of the study and Research methodology forms the contour. This chapter gives a brief understanding of the problem area and upper view of the findings done by various jurists, advocates, authors etc. in this very subject. The second chapter is –'Legal and Techno-Legal Issues in Privacy and Data Protection in e-Commerce'. In this chapter catena of Indian Landmark judgments have been perused in order to understand the concept of privacy and other related rights like, freedom of speech and expression. Cases like *S. Puttaswami (Retd.) (2017)*, *R. Rajagopal vs. State of Tamil Nadu (1994)*, popularly known as the *Auto Shankar case*, *Kesavananda Bharati Case (1973)* etc. are some of the few cases where Supreme Court has discussed the issue of privacy in length. This chapter also incorporates the origin and development of privacy along with the legal issues that exists in the Indian laws. Issues like, zero definition of the term 'privacy' are the main highlight along with different contours of privacy like data privacy, online privacy etc. Different statues like, the Indian Constitution, Information Technology Act, 2000 etc. have also been incorporated which has helped in understanding the existing legal and regulatory issues of privacy and data protection particularly that exists in online platform. The third chapter – 'Legal Framework for Privacy and Data Protection in e-Commerce and International Documents', highlights the concept of privacy and data protection and has tried to understand and analyse it through Indian laws like former Consumer Protection, Act of 1986, The Indian Penal

Code, 1860, Constitution of India, The Information Technology Act, 2000, The Information Technology (Amendment) Act, 2008 etc. This chapter further discusses international documents like, W.T.O., OECD, APEC, WIPO, ECHR, INTERPOL etc. to understand the existing legal framework in India. This chapter in a nutshell tries to point out the lacuna that exists in Indian laws in dealing with the above mentioned issues of privacy and data protection and also moves the focus to the international documents which deals with cybercrimes and cyber attacks way more efficiently than our laws. The fourth chapter – ‘Regulatory Issues Involved In Protection of Privacy and Data Protection in e-Commerce’, in particular discusses the regulatory issues that exists in Indian laws like Code of Civil Procedure, 1908, The Indian Contract Act, 1872, Information Technology (Intermediaries Guidelines) Rules, 2011 etc. The main regulatory issue which has been discussed and forms the crux of this chapter ranges from issues of liabilities of intermediaries/ middleman to issues of choice to law and jurisdiction. International Documents and Organizations like the OECD and TRIPS are also discussed to understand consumer’s data, privacy protection, and safeguard approaches which can be practiced online while engaging in e-Contracts etc. The fifth chapter – ‘Comparative Study of Privacy and Data Protection Laws in e-Commerce’, incorporates, discusses and analyses the evolution of laws on privacy and data between four major countries like U.K., E.U., U.S., and India. In this chapter the main area of research has been done in the approach of these countries in addressing these issues of privacy and data protection. A comparative study has not only led to discovering the prevailing situation in these countries but has also paved a guiding path for a developing country like India to frame their own comprehensive laws to avoid confusion and get rid of scattered laws. The sixth chapter – ‘Conclusion and Suggestions’, have tried to melt down all the observation and conclusion arrived at in

each of the preceding chapters and has also tried to cover topics which could have been omitted unintentionally. Necessary sincere suggestions have also been incorporated in the end of the conclusion to suggest addition, omission etc. in the existing legal and regulatory framework in India.

## CHAPTER ONE

### “LEGAL AND REGULATORY ISSUES OF PRIVACY AND DATA PROTECTION IN E-COMMERCE: AN ANALYTICAL STUDY”

#### 1.1. Introduction

The historical journey of ‘privacy’ in India began with the landmark case of *Kesavananda Bharati v State of Kerala*<sup>1</sup>, which evolved the *Doctrine of Basic Structure*, and pointed out that the power of parliament is limited in the field of amendments concerning Indian Constitution. *MP Sharma Chandra v Satish Sharma*<sup>2</sup> is known to be the first case in Indian history to have discussed the issue of ‘privacy’ and contended that the provision of search and seizure (provided under the Criminal Procedure Code, 1973) to be unconstitutional and violative of Fundamental Rights. Another light on privacy came in the case of *Kharak Singh v State of Uttar Pradesh*<sup>3</sup>, which upheld ‘right to privacy’ as a statutory right only and denied it to be a fundamental one. In this particular case, the Court further went to say that privacy with respect to home is limited and circles around the sphere of personal liberty only and concerning surveillance at public place, there exist no such right.<sup>4</sup> So basically, the Court simply conveyed the message that privacy is protected within walls of home only and is subjected to surveillance once it reaches the public domain. *ADM*

---

<sup>1</sup> AIR 1973 SC 1461

<sup>2</sup> (1954) 1 SCR 1077

<sup>3</sup> (1964) 1 SCR 332

<sup>4</sup> Abhinav Gupta, *Privacy: Whether a Fundamental Right?*3 (Foreword by Prof. Dr. S. Rajendra Babu), “A Public Discourse on Privacy-An Analysis of Justice K.S. Puttaswami v Union of India” (Dr. R. Venkata Rao & Dr. T.V. Subba Rao Edtrs.)

*Jabalpur case v Shivkant Shukla*<sup>5</sup> is marked as the ‘black judgment’ in the career of judicial pronouncement. This case too rejected privacy to be a fundamental right but has played a role in addressing the issue of privacy in India. Later, in the case of *NAZ Foundation v Government of NCT*<sup>6</sup>, the court pronounced dignity and privacy to be the part and parcel of the same right but beautifully denied it to be a Fundamental Right.

The Indian court was flooded by other cases like *I.R. Coelho v State of Tamil Nadu*<sup>7</sup> which upheld the *ADM Jabalpur* case supra to be unwarranted. The term water-tight is associated with number of Indian cases that speaks about the limited nature of privacy as a right under the Indian Constitution. This restricted water-tight theory was supported by the judgments made in *R.C. Cooper v. Union of India*<sup>8</sup>, however *Maneka Gandhi v. Union of India*<sup>9</sup> did not support this theory.

After the perusal of the facts laid down in *Puttaswami case*<sup>10</sup> and reprising the fate it brought in the judicial history by welcoming ‘privacy’ as part of our Fundamental Right, it is not possible to deny the criticism it holds in not recognizing and declaring guidelines for data and information privacy.

The areas which were addressed in this case are about the recognition of right to privacy as a core fundamental right, nature and facets of privacy, restrictions which may have been placed on this right, nature and facets of dignity, Article 21 of the

---

<sup>5</sup> (1976)2 SCC 521

<sup>6</sup> (2014) 1 SCC 1

<sup>7</sup> (2007) 2 SCC 1

<sup>8</sup> AIR 1950 SC 27

<sup>9</sup> 1978 SCR (2) 621

<sup>10</sup> (2017) 10 SCC 1

Indian Constitution, preamble, fundamental rights and constitutional interpretations. In this case, part III of the Indian Constitution and articles like 21, 19, 14, 25 and 28 along with the preamble was referred by the court to understand the intrinsic nature of privacy. Judgments of the Supreme Court in former cases of *M.P. Sharma*, AIR 1954 SC 300 and *Kharak Singh*, AIR 1963 SC 1295 Supra, was also looked into, where the judges declined to hold the right to privacy as a part of the fundamental rights. The decision in the above two cases was that the right to privacy as a right cannot be covered under the constitution. However, the rulings in these two cases were overruled in this *Puttaswamy case* Supra. Another important question discussed in this case was whether the collection of biometric data violated the right to privacy? In deciding this particular question cases like *Gobind*, (1975) 2 SCC 148, *R. Rajagopal*, (1994) 6 SCC 632 and *PUCL*, (1997) 1 SCC 301 were evaluated by the court. Issues of data privacy, profiling, data mining, and data protection regime were also highlighted while addressing privacy issues. The issue of Aadhaar on the question of right to privacy as one of the fundamental right under the Indian Constitution was decided by the court after affirming and referring to numerous cases on privacy, dignity and other contours of fundamental rights.<sup>11</sup>

With the introduction of technology, there has been an unprecedented emphasis on data and information. An increased human interaction in an online platform has paved

---

<sup>11</sup>*Union of India v Bhanudas Krishna Gawde*, (1977) 1 SCC 834, *Prem Shankar Shukla v Delhi Admn.*, (1980) 3 SCC 526, *Francis Coralie Mullin v. UT of Delhi*, (1981) 1 SCC 608, *Bandhua Mukti Morcha v. Union of India* (1984) 3 SCC 161, *Khedat Mazdoor Chetna Sangath v. State of M.P.* (1994) 6 SCC 260, *M. Nagaraj v. Union of India* (2006) 8 SCC 212, *Maharashtra University of Health Sciences v. Satchikitsa Prasarak Mandal*, (2010) 3 SCC 786, *Mehmood Nayyar Azam v State of Chattisgarh* (2012) 8 SCC 1, *National Legal Services Authority v Union of India*, (2014) 5 SCC 438, *Shabnam v. Union of India*, (2015) 6 SCC 702, *Jeeja Ghosh v. Union of India* (2016) 7 SCC 761, *Olga Tellis v. Bombay Municipal Corpn.*, (1985) 3 SCC 545, *Unni Krishnan, J.P. v. State of A.P.*, (1993) 1 SCC 645, *Maneka Gandhi v Union of India*, (1978) 1 SCC 258, *Golak Nath v. State of Punjab*, (1967) 2 SCR 762, *Kesavananda Bharati v State of Kerala*, (1973) 4 SCC 225, *Indira Nehru Gandhi v Raj Narain*, 1975 Supp SC 1, *Minerva Mills Ltd. v Union of India*, (1980) 3 SCC 625, etc.

way for privacy protection and therefore is of a grave prime concern. The generation of huge amount of data online and its vulnerability to being misused have created a new challenge both in terms of legal and regulatory ones. With the presence of considerable amounts of data on the internet, the issue of privacy intrusion has increased enormously. Therefore, in these circumstances, the need for privacy law can hardly be overstated.<sup>12</sup> In contemporary society, the internet and technology have attained prominence in everyone's daily life and because of the damage done by the internet to our personal space and data, people have become conscious of these rights like never before. Also with the generation of sensitive personal data in a bulky amount by the conscious or unconscious activities of people in everyday activity the lives of people has invited additional vulnerability.<sup>13</sup>

The classical legal definition of privacy is attributed to Judge Cooley (United States judge), who defined privacy as '*the right to be left alone*'<sup>14</sup> almost certainly the best-known definition of privacy so far. The right to privacy and data protection is vital in e-Commerce and is interconnected with security and trust which are two of the crucial problem of e-users in e-Commerce platform. Over the years, the privacy protection for e-users transactions has turned out to be very vital. Legal issues in e-Commerce include issues of lack of legal definition of the term privacy, data privacy and other issues consists of inefficiency of the present Indian laws in dealing with e-Commerce problems. The other issue involves techno- legal and regulatory. All these issues are discussed in length in the succeeding chapters.

---

<sup>12</sup>Rishika Taneja and Sidhant Kumar, *Privacy Law, Principles, Injunctions and Compensation* 231(EBC Publishing (p) Ltd., Lucknow) (Printed by, Gopsons Papers Ltd., A-2, Sector-64, Noida) (1<sup>st</sup> Edn. 2014).

<sup>13</sup>*Ibid.*

<sup>14</sup> Ian J. Llyod, *Information Technology Law* 17 (Published by, Oxford University Press 198 Madison Avenue, New York, United States of America) (Printed in, Ashford Colour Press Ltd, Gosport, Hampshire) (7<sup>th</sup> Edition, 2014).



In India the Supreme Court had tried to cover the term ‘privacy’ in number of cases, *Maneka Gandhi*<sup>15</sup> and *Gokal Prasad v Radho*<sup>16</sup> are two of the best example. Despite of the laws like Information Technology Amendment Act, 2008 (ITAA), which provides for legal recognition of business conducted over the internet, with numerous sections providing for the protection as well as punishment in case of failure and omission in respect of e-Commerce activities, over the years thinkers, research scholars and people at large are over burdened with the issues of privacy and data protection in the internet world. Despite several amendments which have modified as well as has included new or additional sections to provide a comprehensive law governing e-Commerce, it has miserably failed to give a precise and universally accepted definition of the term ‘Privacy’ and ‘Data Privacy’ and as such, has generated a concern and need for having a comprehensive law for providing a set of definitions of the term ‘Privacy’ and ‘Data Privacy’, in short, a privacy law.

To address new arising threats to privacy and data protection in e-Commerce, comprehensive law is the only expected relief for curbing the legal, techno- legal and regulatory issues in e-Commerce.

The right to privacy is infringed by many factors<sup>17</sup> and in the absence of even one legal definition of this term, the concern for its protection becomes even more important. The term “privacy” is connected with other terms too, and in order to

---

<sup>15</sup> 1978 SCR (2) 621

<sup>16</sup> (1888) ILR 10 All 358

<sup>17</sup> The right to privacy is infringed by many factors –

- (i) Utilizing private data already collected for a purpose other than that for which it was collected;
- (ii) Sending of unsolicited emails or spamming or spam;
- (iii) Spimming;
- (iv) Adware and Spyware;
- (v) Phishing;
- (vi) Unauthorized reading of emails of others.

expound it, it becomes necessary to incorporate and understand the definitions of those terms which are in nexus with the parent term “privacy”. Such terms are integrated into different succeeding chapters according to the need and necessity.

Talking about data protection numerous questions are unheard and unaddressed. To list some, it includes questions like; what types of data are to be regulated? What sorts of activities over the internet are regulated? Are Internet Service Providers, Controllers and users of websites classed as data users or computer bureau operators? What are the obligations of registration for internet data users and computer bureau operator’s operating in India as well as abroad, when there are no laws on Data Protection? With the internet often lacks security, what are the principles for adequate data security over the internet? How to protect data which travels within India and those data which flows overseas? Technology has affected personal privacy and is repeatedly influencing our understanding of the notion of privacy.<sup>18</sup> The concept of privacy differs from person to person and by considering the taxonomy of privacy in relations to numerous forms, we could get through the haziness surrounding the concept of ‘privacy’.

The Central setback in legal and regulatory issues of privacy and data protection in e-Commerce is manifold. Legal issues mean the issues in laws; these laws are the products of written statutes, passed by legislatures. Regulations, on the other hand, are standards and rules adopted by administrative agencies dealing with the enforcement of such laws.

---

<sup>18</sup>Rahul Matthan, *Privacy 3.0 Unlocking our Data-Driven Future* 15 (HarperCollins Publisher) (Printed at Thomas Press (India) Ltd.)(2018).

## 1.2. Privacy

*“No technology has ever been shut down because of the privacy threat it posed to the existing social order”<sup>19</sup>*. The word privacy is not defined by any laws to date. This right was not absolute earlier but today this right is recognised as a right and has formed an integral part of Article 21 of the Indian Constitution. Privacy as a concept differs from person to person and is protected differently in different countries. In India, this right under the Information technology Act is not defined but is infringed on numerous occasions when an individual is engaged in e-Commerce and other activities online and in other social platforms facilitated by the internet. Due to the technological swift, this basic human right is infringed by many factors. Private data forms part and parcel of privacy and infringement of one may affect the other.

Privacy is related to individual while cybersecurity, on the other hand, is more complex and includes the entire ecosystem. Privacy also involves security issues and involves dimensions like, (i) integrity which means prevention against unauthorized data modification, secondly, (ii) non-repudiation which refers to prevention against renegeing on an agreement by the party involved, (iii) authenticity i.e., authentication of data source,(iv) confidentiality is the protection against unauthorized data disclosure. Other issues akin to e-Commerce include tracking activities of consumers by using web cookies, web bugs, denial of service (DOS) attacks, data mining, breach of confidentiality, and validity and binding nature of e-Contracts in online transactions, etc.

---

<sup>19</sup>Rahul Matthan, *Privacy 3.0, Unlocking our Data-Driven Future* 26 (HarperCollins Publishers, India) (2018).

Definition of the term 'privacy' varies owing to a different situation such as background of a society or environment and as such in an international arena of all the human rights; privacy is regarded as the most difficult one to define. Some countries read this concept of 'privacy' along with the concept of 'data protection' while other interpret it in terms of personal information. Scholars and writers in the past had regarded privacy rights as one of the basic Human Rights and now in this digital age, it has become one of the most important issues. Every country has embedded the privacy rights in their Constitution and this right is also well addressed and protected under the Universal Declaration of Human Rights (UDHR), and in International Covenant on Civil and Political Rights (ICCPR), as well as in many other international treaties.<sup>20</sup> Privacy has also been recognized in the Quran and many references are also found in Jewish law and the Bible too. The technologies have given a weapon to eavesdroppers to invade into the privacy of individuals and as a fact; the concern for privacy is at greater risk than it was in the past. The use of numerous data by computers and internet which commodify the data regarding individuals are in a way violating the individual's privacy <sup>21</sup>and thus this legal and techno-legal issue needs to be addressed not only at the National level but at the International level too because of the simple fact that 'internet knows no boundaries'. The global consent on adopting a bench definition of the term 'privacy' is yet to achieve. Legal protection for privacy existed in western countries for hundreds of years.<sup>22</sup> Privacy in Indian history speaks about our forefathers who abhorred the idea

---

<sup>20</sup> A. Kranthi Kumar Reddy, *et.al.*, *Cyber Space and the Law-Issues and Challenges 202* (Published by, NALSAR University) (Printed at, the Print House, Hyderabad) (2004).

<sup>21</sup>Raman Mittal and Neelotpal Deka, *Cyber Privacy, Legal Dimensions of Cyberspace 197* (S.K. Verma & Raman Mittal, Eds.), Indian Law Institute.

<sup>22</sup> In 1361, the Justices for Peace Act in England provided for the arrest of peeping toms and eavesdroppers. (*Eutick v Carrington*). William Pitt (1763), in his speech on the Excise Bill, British Parliamentarian wrote, "The poorest man may in his cottage bid defiance to all the force of the Crown. It may be frail; its roof may shake; the wind may blow through it; the storm may enter; the rain may

of seclusion. They conceived privacy as against their safety, as demanding privacy would mean threat to their lives. The more they asked for privacy, more they were under risk of losing their lives. They believed in giving away one's privacy for the betterment of whole. This concept of 'privacy', free from intrusion, having control over one's personal information etc. came only after the development of web network. With passing time, society understood the concept of privacy, and desired to keep their life private, free from interference. They started guiding themselves against intruders who invaded into their personal lives without their consent. This desire gained momentum after the menace technology gave in the form of 'cookies', 'web-bugs', 'data theft' etc.

In India, privacy, as a right got momentum after the Government initiative in the year 2017 to provide a Unique Digital Identity (UID) to the people living in the Country (i.e. 1.3 billion people). Linkage of Aadhaar was then made mandatory to avail schemes like LPG and SIM cards, Banks etc. The ubiquitous nature of Aadhaar was opposed to the basic right of human privacy as people were made to link their Unique Digital Identity with the banks as well for availing of the services. People's mobiles were flooded with the messages asking for linkage of their Aadhaar. In the absence of privacy law in India, it was tough to protect the same in a full –fledged way.

The dynamic nature of technology has highly influenced the notion of privacy and data and has automatically raised a question on its regulation in the absence of privacy law. A healthy balance between the perks of technology and privacy has become a myth as there is no law to protect the same on the occasion of its infringement in

---

enter-but the King of England cannot enter; all his force dare not cross the threshold of the ruined tenements”.

---

online jurisdiction. Technology has gradually entered into our private space and will continue to do so if not checked properly with the privacy laws.<sup>23</sup>

According to Rahul Matthan,<sup>24</sup> privacy has gone through three distinct phases of evolution, where the first phase of privacy was developed by human beings for personal space and private thoughts. Secondly, laws were made to protect the information people shared with other fellow beings and thirdly with the introduction of technology in human lives. Among the three phases of evolution of privacy, the last one is the most dangerous. Technology has widened the circles and has allowed strangers to enter our personal space from anywhere. The traditional consent-based protection of privacy which served for many decades is indisputably ineffective in this contemporary technological driven society.

There has been an ironic change in human behavior towards the concept of privacy, as what was abhorred by our forefathers is highly valued today. This change has been mostly due to the entering of technology in our private personal space. The idea of self and having a distinct identity from the community started because of the technology. The modern notion of privacy is borne out of the human anxiety to develop the society with the help of technology. The influence of these technologies has been so much so that our private space, personal information, and personal data are under the continuous threat of being misused.

It is important here to mention that as per Rahul Matthan Supra, the author of the book titled “Privacy 3.0”, the concept of privacy as a legal right was not first

---

<sup>23</sup>Rahul Matthan, *Privacy 3.0, Unlocking our Data-Driven Future*, (HarperCollins Publishers, India) (2018).

<sup>24</sup>Author of the book “Privacy 3.0” (2018).

recognized and defined by Warren and Brandeis as thought by almost all of us, but according to him this concept of privacy was firstly developed by James Madison, one of the architects of the American Constitution, who had articulated right to privacy before Warren and Brandeis but found it difficult to express in the language of the times. He stated this right as a sacred form of property that needed to be given the status of a natural and inalienable right.<sup>25</sup>

### **1.3. Data**

Data Privacy law has long been afflicted by an absence of clarity over its aims and conceptual foundations. Although section 2, sub-section 1 clause (o) of the Information Technology Act defines ‘Data’ but ‘Data Privacy’ and ‘Personal Data’ is not yet defined. Apart from this section, there are section 43 and section 66 of the Information Technology Act 2000, which provides Civil and Criminal liability i.e. penalty and compensation for damage to computer, computer system, etc. and other computer related offences respectively. The question here arises is that of ‘what constitutes Personal Sensitive Data? Although India has RBI guidelines that provides additional authentication on a system which are based on information encrypted, the guidelines however are limited to the banking sector only and hardly covers any mandates relating to failure to protect personal data and information in e-Commerce online transaction.

### **1.4. e-Commerce**

Electronic Commerce makes it possible to do any kind of business in a very simple way. What makes it simple is the problem, which is faced by e-Users. The actual

---

<sup>25</sup> Rahul Matthan, “Privacy 3.0, Unlocking our Data-Driven Future” 43-44, (HarperCollins Publishers India) (2018).

reason for this simplicity in e-transaction is the lack of existing legal frameworks and weak enforcement mechanisms.

In the absence of uniform worldwide law for e-Commerce, while shopping on the Internet, most people typically do not know about what is happening in the background. Customer information has to pass through several hands, so the safety and security of a customer's personal information lie within the hands of unidentified people. Major issues regarding the legalization of electronic transactions include ensuring proper online contracts, recording retention obligations, and foreign data protection law. Electronic transactions are different from traditional type of businesses. When a transaction takes place, the problem arises in terms of 'who has jurisdiction?' and 'who has the authority to apply law over the transaction?' For example, if a person buys a laptop on a local store, he knows his legal rights and if the computer does not work after taking it home, and the store refuses to settle up, then he can probably take the dispute to his local small claims court. But if the person buys the computer online, from an online vendor who resides in the other side of the world through a dealer who is based in another country then the enforceability of his right becomes a serious issue in the absence of clarity. The problem is which country's protection laws will apply? Without knowing which particular set of laws apply, it is impossible to know whom to sue. Security involving the privacy of a user's data is always one of the main concerns while doing business online.

Electronic Commerce (E-Commerce) is overburdened with number of factors like the fear of intruders who can with the help of technology, on having opportunity to cause harm, such harm can appear both at the national and international level. In such a case



absence of a comprehensive law leads to uncertainty and makes the circumstances more complex.

### **1.5.Choice of Forum**

With the introduction of Information Technology Act 2000, some changes in other traditional laws were made. For instance, under the Evidence Act, section 65 A (**Special provisions as to evidence relating to electronic record**) was inserted along with section 65 B (**Admissibility of electronic records**), which provides for evidence related to electronic records. There exists no convenient forum to file a suit for infringement, taking place during or after online e-Commerce transaction. The problem lies in protecting the privacy of e-users in e-Commerce transaction because in the absence of a comprehensive law to protect the rights and privacy of e-users in online transaction, mere hosting of a website which can be accessed by anyone from any jurisdiction, is considered to be in-sufficient for the purpose of jurisdiction and claiming rights in cases of infringements which occurs on an online platform.

### **1.6. Choice of Jurisdiction**

The question of jurisdiction in e-Commerce was attempted by the court in *World Wrestling Entertainment vs. M/S Reshma Collection & Ors.*<sup>26</sup> The problem was that of territorial jurisdiction of the Court in entertaining the suit, Court observed that "As a matter of fact in a matter where services are rendered through the domain name in the internet, a very alert vigil is necessary and a strict view is to be taken for its easy access and reach by anyone from any corner of the globe.

---

<sup>26</sup> FAO (OS) No. 506 of 2013.

### **1.7. Statement of Problem**

The Central setback in “Legal and Regulatory issues of Privacy and Data Protection in e-Commerce” is manifold and Legal issues means the issues of laws and laws are the products of written statutes, passed by legislatures whereas, Regulations, on the other hand, are standards and rules adopted by administrative agencies that govern how laws will be enforced. The research problem is framed to examine the legal and regulatory challenges of Privacy and data protection which e-Commerce is facing hence the Statement of problem has been divided into four parts. First part deals with the issue of lack of proper legal definition of the term Privacy and Data privacy, and e-Commerce along with difficulty in formulation of the definition etc. The second part deals with the needs and justification of privacy and data protection in e-Commerce transaction. Third part covers the Regulatory issues like liability of third party etc, while the last part deals with the Technical issues like cookies etc, involved in the protection of Privacy and Data Privacy in e-Commerce Transaction.

The first and foremost problem that lies in the area of Privacy and Data Protection is, there is not a single uniform definition of the term ‘PRIVACY’ and nowhere the term ‘Privacy’, ‘Data Privacy’ along with ‘e-Commerce’ has been defined in any Acts, except the Supreme Court which made an attempt to incorporate the word ‘Privacy’ in the light of Article 21<sup>27</sup>. In India till date there exists no legislation that advocates the Privacy Rights of an Individual or Organization against private parties in e-Commerce transactions. Even though section 72A (Punishment for Disclosure of information in breach of lawful contract) of the Information Technology Act, 2000 with Amendment (2008) prescribes punishment for an offence of disclosure of information to another

---

<sup>27</sup> No person shall be deprived of his Life and Personal Liberty unless except the procedures established by Law.

entity without the consent of a member, the aforementioned Act does not prescribe as to 'What Constitutes Personal Information' in e-Commerce transactions. E-Commerce (Electronic Commerce) is overburdened with the threats from anyone with the capability, technology, opportunity, and intent to do harm, these Potential threats can be foreign or domestic, internal or external, state-sponsored or a single rogue element. In such a case absence of a comprehensive law leads to uncertainty and makes the circumstances more complex. Data Privacy law has long been afflicted by absence of clarity over its aims and conceptual foundation. Though section 2, sub-section 1 clause (o) of the IT Act defines 'Data' but 'Data Privacy' and 'Personal Data' is not dealt by the Act. Apart from this section, there are section 43 and section 66 of the ITA 2000 which provides Civil and Criminal liability i.e. Penalty and Compensation for damage to computer, computer system, etc. and Computer Related Offences respectively. The question here arises is that of 'what constitutes Personal Sensitive Data? Though India has RBI mandates on a system providing additional authentication based on information encrypted on the cards, such guidelines are limited to Banking sector only and hardly covers any mandates relating to failure to protect Personal Data and Information in e-Commerce online transaction. The Problem in e-Commerce is that of protection of Privacy and Security, as since the Internet is an open system, details of its underlying technologies are freely available to anybody. This means that the way data passes through the Internet is in the public domain; the consequence of this is that, theoretically, anyone with the right tools can eavesdrop on data passing from one computer on the Internet to another. And in the absence of any comprehensive Data Protection law in India and no proper single definition of the term 'Data Privacy', it becomes very difficult to safeguard privacy and protect security in the borderless e-Commerce transaction. The Regulatory issues

in Privacy and Data Protection includes, issues of Security and Uninterrupted login in e-Commerce over the internet incorporates issues of Dissemination of sensitive and confidential medical, financial and personal records of individuals and organizations; sending spam (unsolicited) e-mails; tracking activities of consumers by using web cookies; and Unreasonable check and scrutiny on an employee's activities, including their email correspondence. The question is as to who will decide the liability arising out of such unreasonable check and scrutiny, tracking of activities by use of web cookies etc? , and what constitutes the nature of such liabilities? There is no law in India to handle such questions. The issue in e-Commerce also covers issue of Security. Though the 'Indian Contracts Act' and 'The Information Technology Act' deals with subject of Data Protection, these laws does not deal with utility values as it is dealt in countries like U.S.A. Despite of the effort made by passing of a 'Personal Data Protection Bill in 2006' for having a Personal Data protection law as a separate discipline, till now it has not been passed by the Houses of the Parliament and there is uncertainty as to whether it will become an Act or not. In such situation the issues relating to Data security, theft and sale of stolen Data in e-Commerce will be further triggered, leaving behind the question as to which law will deal with such issues of data stealing etc.

Electronic Commerce makes it possible to do any kind of business in a very simple way. What makes it simple is the problem, which is faced by e-Users. The actual reason for this simplicity in e-transaction is the lack of existing legal frameworks and weak enforcement mechanism.

In the absence of uniform worldwide law for e-Commerce, while shopping on the Internet, most people typically do not know about what is happening in the

background. Customer information has to pass through several hands, so safety and security of a Customer's personal information lies within the hands of the business. Major issues regarding the legalization of electronic transactions include ensuring proper online contracts, recording retention obligations, and foreign data protection law. Electronic transactions separate from traditional type of businesses. When a transaction takes place, the problem arises in terms of 'who has jurisdiction?' and 'Who has the authority to apply law over the transaction?' For example, if a person buy a laptop on a local store, he knows his legal rights and if the computer does not work after taking it home, and the store refuses to settle up, then he can probably take the dispute to his local small claims court. But if he buy the same computer online, from a vendor online from the other side of the world, perhaps through a dealer based in yet a third country then the enforceability of his right becomes a serious issues in the absence of clarity. The problem is which country's protection laws will apply? Without knowing which particular set of laws apply, it is impossible to know whom to sue. Security involving the privacy of a User's Data is always one of the main concerns while doing business online. The question of jurisdiction in e-Commerce was attempted by court in *World Wrestling Entertainment v M/S Reshma Collection & Ors.* The problem was that of territorial jurisdiction of the Court in entertaining the suit, Court observed that "As a matter of fact in a matter where services are rendered through the domain name in the Internet, a very alert vigil is necessary and a strict view is to be taken for its easy access and reach by anyone from any corner of the globe." I.T. Act 2000 came with changes in other traditional laws. Hence the Evidence Act which was inserted with the section 65A (**Special provisions as to evidence relating to electronic record**) and section 65B (**Admissibility of electronic records**), which provide for evidence related to electronic records, there exist no

convenient forum to file a suit for infringement, taking place during or after online e-Commerce transaction. The problem lies in protecting the Privacy of e-Users in e-Commerce transaction because in the absence of a comprehensive law to protect the rights and privacy of e-Users in online transaction, mere hosting of a website which can be accessed by anyone from any jurisdiction, is considered to be insufficient for the purpose of jurisdiction and claiming rights in cases of infringements which occurs on an online platform.

The Intermediaries Guideline Rules 2011, runs under the IT Act (Amended 2008) where intermediaries are said to be under obligation to publish the rules and regulations, privacy policy and user agreement for access or usage of the intermediary's computer resource by any person. Further it provides for disclosure to the users of computer regarding rules and regulation. However, despite of such guideline there have been cases. Pertinent to refer Consim Info Pvt. Ltd vs Google India Pvt. Ltd, Reed Elsevier, Inc. vs. Innovator Corp., Metaspinner Media GmbH vs. Google Deutschland, LG Hamburg, and Nemetschek AG vs. Google, LG Munich where the court has refused to order third party infringement. Here the problem is that of liability of intermediaries in e-Commerce transaction.

Another issue is that of Cross border e-Commerce jurisdiction. For instance if a person residing in place A buys something online from a company in place B and if any problem occurs after the completion of e-transaction then the question arises regarding where to file the suit ? The IT Act is well applied in extra territorial cases, but is not strong enough to implement its decision on the foreign party. The court possesses no power to bring the foreign party to India for trial. Even if the IT Act

provides for extra- territorial operation i.e., even a website outside India could be penalized for publishing misrepresentation. For e.g. if a company website of country A displays misinformation about the Indian Company i.e. B, then company A could be sued under Indian law, and possibly in the country B. The actual problem lies in the choice of forum, and choice of law as there is no comprehensive law to govern the Trans-border e-Commerce issues of Privacy and Data Protection. Despite of having IT ACT 2000, where section 12 provides for Acknowledgement of Receipt, the problem here lies in how to determine the acknowledgement of an electronic record when the originator do not agree with addressee regarding acknowledgement of receipt? The legal issues here arise in matters of recognizing e-contracts. Another question involving legal issues is that of How to determine the acknowledgement of an electronic record when the originator has not agreed with addressee regarding acknowledgement of receipt? In the case of The United States, *Corinthian Pharmaceutical Systems Inc. v. Lederle Laboratories*, an “order tracking number” issued by an automated telephone ordering system was found to be merely an acknowledgment of the order, rather than an acceptance which formed a binding contract. Applying the same reasoning to common electronic commerce practices, this could mean that a computer-generated message acknowledging receipt of an electronic order may not be sufficient to create a binding contract. The purpose of the message may be solely to confirm receipt of the order. It does not necessarily signify acceptance and e-Users in e-Commerce transaction are not secure in the absence of a clear Act determining the acknowledgement of order and this may in return cause e-Users to lose trust in e-Commerce transaction.

In this regard the problem of Cyber stalking is very much relevant because a user of the Internet finds the details of another user's e-mail account and harasses them electronically, sending them e-mails, contacting them via newsgroups and intruding into the chat rooms that they use and the problem is that India has no such Act which provides liability or defines the term 'Cyber Stalking' and as such there is no relief in cases of infringement of e-Users Privacy and their Data. Even though Data mining has attracted significant interest especially in the past decade with its vast domain of applications but from the security perspective, Data Mining has been shown to be beneficial in confronting various types of attacks to computer systems but at the same time this technology can also be used to create potential security hazards. The question here is Data mining related with e-Commerce? Is Data mining a legal practice in India? Is Data Mining legally permitted in any other Countries? And lastly if it permitted who will be held responsible? Though Cookies are an essential part of the Internet and its absence matters a lot in e-Commerce, there is a growing trend of malicious cookies. Third party Cookies affect privacy and e-Commerce. Cookies are malicious as they watch our online activity and advertise our personal interest and information without our consent to an advertising company who use our profile to target us with interest specific adverts.

### **1.8. Literature Review**

A fairly significant body of research literature exists in the domain of e-Commerce but there is no single Literature to provide a comprehensive analysis and solution of legal, techno-legal and regulatory issues of 'Privacy' and 'Data Protection' in e-Commerce transactions. A selected number of articles, books, journals and available materials from the various online & offline sources are reviewed. Accordingly the



whole literature review is divided in two parts. The first part deals with finding of a definition of privacy and data privacy, formulation of definition, kinds, ingredients, and need and justification of privacy and data protection in e-Commerce transaction. The second part is supplied with technical issues that triggered the problem.

When tracing back to history of privacy and data privacy countries like India and some other like UK & USA even other also around the globe had felt the need for protection of Privacy and Data even in e-Commerce. Privacy is not a part of any legislation, though an attempt has been made by various Jurists, Writers and Authors to define the term 'Privacy'. Data protection and privacy rights are considered to be two of the most important rights conferred by any civilized nation. (Perry4Law). In the digital world some Author is of the view that Internet is a severe threat to privacy, (Aaron Schwabach, 2006) where some view Privacy as Right of Individuals and Organizations to be left alone and secure their personal papers and data (Dr Sherif Kamel, 2008). Freedom from unauthorized intrusion (Anthony Ferraro, 1998) and lack of standard definition of Privacy has thought to be a 'difficult notion' (Adam Moore, 2008). In the e-Commerce era privacy has formed an integral part thereby increasing trustworthiness and loyalty (Eamonn O' Raghallaigh, 2010) and there is a legal requirements for undertaking e- commerce in India which involve compliance with other laws like contract law, Indian penal code, etc.( Edward Elgar) .In the deficiency of a uniform definition of the term 'Privacy' it's protection and that of Data is assumed to be derived from laws like Information Technology, Intellectual Property, Contractual Relation Crimes and Contractual relations. (Bijan Brahmhatt, 2010). With the passage of time the e-Commerce user became aware of the vulnerability of their Data and started changing their password again and again or at

reasonable interval of time due to the issues of Privacy. (Christopher Allen, 2005). Another problem involves new threats to individual privacy as Technology designs people's relationships with Social Institutions (Philip E. Agre, 1997). What had worried the nineteenth century was again observed in the present digital world for posing threats to not only Privacy but too many other areas of laws also (Aaron Schwabach, 2006). Privacy has been classified as Defensive Privacy, Human Right Privacy, Personal Privacy and lastly the Contextual Privacy (Christopher Allen, 2005) Other classification includes state of being alone and remote as well as closeness with the family and friends (Darhl M. Pedersen, 1999) in addition to this there are different layers of privacy which includes a person's privacy, and privacy relating to their behavior , acts, thoughts, feelings, data privacy, communication privacy, etc., (David Wright, 2001).With the development of Technology, complexity of Privacy issues in legal, social-psychological, economic or political has been inadequate and satisfactory. Due to fact that there is not a single uniform accepted definition of the term 'Privacy', States across the globe seeks to balance an Individual's Right to Privacy (Julia Drake) and due to the fact that the concern for Privacy is not new it has concerned almost all the world democracies since 1960 and as such it creates a concern for protecting Privacy and Personal data involving co-operation between countries. (Edward Elgar, 2008). In order to secure freedom of the press States has recognized four different Forms of invasion of Privacy namely intrusion, public disclosure, false light and appropriation. After the legal issue which is involved in defining the term "Privacy", e-Commerce is overburdened with another major setback relating to malicious use of sensitive Personal data (Anastasia, 2015) as well as problem relating to providing Data Security. Other problem incorporates understanding and defining of Sensitive Data, which is not yet attempted by any law

throughout the globe. Aim to minimize intrusion into one's privacy (Vijay Pal Dalmia, 2011) in the process of collection, storage and dissemination of personal data was also figured out by some of the Authors in considering issues relating to Privacy, Data Privacy and its protection. Breach of Private rights of an individual's (Justice Yatindra Singh, Fourth Edn. 2010), from a Computer data containing personal information was considered by the 2008 Amendment Act by inserting Sec 72 and Section 72A for redressing this problem. Issues of Data mining and confidentiality (Stephen E. Fienberg, 2006) relating to e-Commerce was considered to be front and center along with threats to privacy (Aaron Schwabach, 2006) in the Internet. Use of the text files called cookies in collecting data from users for marketing them in advertisements networks and third party websites with the help of JavaScript and flash technologies has said to have taken advantage for not having one unified body which could have govern the online space with its strict and stringent rules (Sowmyan Jegatheesan). New age has also come up with issues of security (Don Tapscott) along with new threats to privacy and its protection (Daniel J. Solove, 2006). In understanding the legal and techno-legal issues of Privacy, Data Privacy and Data Protection in e-Commerce understanding of the laws of other Nation Country is vital. Obligation on Data Controller, transfer of personal Data, Data Protection (Vinod Bange et al, 2012) has been the rule set out in the U.K.'s - Data Protection Act of 1998. Right to Privacy is viewed as an independent concept (Thomas I. Emerso) by some Authors as this concept of Privacy made first appearance in America law as a tort, a civil suit for damages or an injunction to protect against an unwarranted invasion by others of the vague "right to be let alone". Privacy Commissioner for Personal Data of Honkong has incorporated six data protection principles aiming to protect the privacy of individuals in relation to their personal data. (Roderick B. Woo,

2006) and this ordinance was viewed as a cornerstone in the creation of a new culture in carrying out and in handling of personal data during their whole life cycle from their collection to their destruction. In the age of information some Author viewed the massive collections of data stored on disparate structures as unfortunate as it created initial chaos and led to the creation of structured databases and database management systems (DBMS). (Osmar R. Zaïane, 1999). In Countries like U.K., apart from the legal issue, other techno-legal issues were also discovered like that of Cookies in e-Privacy Directive (W. Gregory Voss, 2012). Difficulty in defining the term ‘Privacy’ among all the Human Rights has been identified in the international catalogue. (C.M. van der Bank, 2012). Data protection has been considered to be no longer just a Privacy right, as data have also become an economic good, which means it also is property. The issues of the ‘traffic data’ are also crucial in such a scenario as this can be used against the person and can lead to make assumptions about what type of person is he and what advertising might be of his interest. the person in internet is paying for the information he wants to collect but the privacy intruders are using his money for their economic benefits while using his traffic data for the collections of his liking and disliking in order to sale whatever they want. (Access International).

Another issue is privacy protection laws which are different in different countries. The difference in laws becomes more problematic in cross border disputes. Hence this raises complication in privacy compliance processes. (W. Gregory Voss et al, 2013). The Author around the globe is also concerned with the regulatory issues and legal questions that have alarmed the online activity due to growth of increased internet and its boundary-less activities (M. Ali Nasir, 2014).Some Author views privacy and security as still ongoing research problems and regards tackling of privacy, as a

difficult matter. Issues like jurisdictional conflicts involving States, private actors, and regulatory agencies in the global economy(Christopher Kuner, 2010) has been highlighted to be interconnected and regarded the internet as ubiquitous. States also frequently assert their jurisdiction over conduct occurring outside their own territory, particularly with regard to conduct on the Internet. Reserve Bank of India introduced guidelines governing internet banking, confidentiality, anti-money laundering and know-your-customer norms, which may have prompted customers to move towards the e-platform, albeit with some concerns with respect to the privacy and security of their banking transactions. (Kartik Maheshwari et al, 2012). To understand the concept of privacy some Author have found that having a fair attitude towards neutral privacy will help in identifying intrusions into private space of an individual. And secondly thinks that there should be a consistency in the privacy to attach its value for in claiming the legal protection and lastly states that privacy must be a concept useful in legal contexts, a concept that will enable to identify those occasions calling for legal protection, because the law does not interfere to protect against every undesirable event. (Ruth Gavison, 1980) The Protection of Privacy Rights from Government Action in e-Commerce is required (Nishith Desai & Praveen Nagree) as well as there is a need for proper recognition of the problems relating to acknowledgement issue in e-Commerce. (*Bhanu Srivastava 2015*) and the concern is *much more in America* with regard to online tools, where the Americans has expressed a consistent lack of confidence about the security of everyday communication channels and the organizations that control them and they exhibited a deep lack of faith in organizations of all kinds, public or private, in protecting the personal information they collect (Missbaron 97, 2017).

## **1.9. Rationale and Scope of Study**

The rationale behind this study is to analyze the research objectives, research question as well as a hypothesis to understand the legal and regulatory issues of privacy and data protection in e-Commerce. The analysis of different contours of privacy read together with data and the absence of privacy laws in India is interesting to understand the prevailing legal and techno-legal issues in the e-Commerce forum. The critical study of privacy and data issues in a technologically driven society is a gateway to understanding many other inevitable issues like choice of law, choice of forum and jurisdiction. The study is not only limited to India but extends to other three major developed countries which include the U.K., E.U., and the U.S.A. The concept of privacy no doubt differs from person to person and each country has got their own legal and regulatory ways to deal with the same but having a comparative study between these four technologically affected countries will surely help to understand the problem from its roots and will help the young scholars, privacy advocates, and even the Governments to come up with the effective solutions and come up with comprehensive privacy and data laws.

## **1.10. Research Objectives**

1. To study the issues, arising in respect of Privacy and Data Protection in e-Commerce in India and to critically identify the deficiencies in the current framework of e-Commerce Regulations in India and investigate requisite amendments.
2. To analyze the grey areas on the imposition of liability on the intermediaries in matters relating to issues concerning privacy and data protection in e-Commerce- in India as well as in cross- border e-Commerce

3. To study and analyze the problems of tracking activities done by cookies, data mining and issues of security and uninterrupted login in e-commerce faced by e-consumers and their prospective solutions.

### **1.11. Research Questions**

1. What are the issues, arising in respect of Privacy and Data Protection in e-Commerce in India and the deficiencies in the current framework of e-Commerce Regulations in India?
2. What are the grey areas on the imposition of liability on the Intermediaries in matters relating to issues concerning privacy and data protection in e-commerce- in India as well as in cross- border e-Commerce?
3. How far the problems of tracking activities done by cookies, data mining and issues of security and uninterrupted login in e-commerce faced by e-consumers and their prospective solutions?

### **1.12. Hypothesis**

1. Existing laws in e-Commerce are not adequate to address the legal and technological issues of Privacy and Data Protection.
2. There is a no due care liability of the service provider for the data protection

### **1.13. Research Methodology**

The entire research is purely doctrinal. It is descriptive and analytical by nature. The research is based on primary sources, includes Statutes, Laws, Regulations and, Acts. Secondary sources include materials from articles, research reports, policy papers, government documents, etc. The researcher has focused on various Indian judgments

as well as of other countries to have a clearer insight into the research objectives, research questions, and hypothesis.



## CHAPTER TWO

### LEGAL AND TECHNO-LEGAL ISSUES IN PRIVACY AND DATA

#### PROTECTION IN e-COMMERCE

##### 2.1. Introduction

The most crucial legal problem has been in defining the term privacy. The term privacy lacks a legal definition but after a decade of struggle in defining this hazy term the judgment in the *Puttaswami case*<sup>28</sup>, *Supra* chapter 1 covered it as a right under Article 19 and 21 of the Indian Constitution. The journey was not easy as several landmark cases had to go through critical scrutiny before this expression found its place as one of the fundamental rights. India was not done with praising the judicial pronouncement brought in the *Puttaswamicase* that to our utter dismay, on 28<sup>th</sup> July 2018, Telecom Regulatory Authority of India's (TRAI) Chairman RS Sharma published his Aadhar no. online, challenging anyone to do any harm to him. Challenge was accepted by the so-called "ethical hackers", who all in less than a day was shockingly and embarrassingly successful in taking out his personal information<sup>29</sup> (TRAI's Chairman)<sup>30</sup>.

---

<sup>28</sup>*S. Puttaswami (Retd.) and Ors. v Union of India and Ors* (2015)8 SCC 735

<sup>29</sup> Voter ID number, telecom operator, phone model was made public on Twitter. Not just that, Twitter user Anivar Aravind (along with a few others) even manage to send Re 1 to RS Sharma's bank account via electronic bank transfer. This is after some of the hackers claimed to access to Sharma's bank account number and IFSC code for several banks. The ethical hacker claimed to send Mr. Sharma the princely sum of Re 1 in the hope the Aadhar system implemented "better engineering to protect user privacy", available at <https://timesofindia.indiatimes.com/india/hackers-deposit-re-1-in-trai-chiefs-account/articleshow/65190556.cms> (Last visited on July 31, 2018).

<sup>30</sup> "Aadhar", available at <https://www.indiatimes.com/technology/news/after-aadhaar-leak-hacker-deposits-rs-1-in-trai-chairman-s-account-to-improve-system-s-privacy-350316.html> (Last visited on July 31, 2018).

After the perusal of the facts laid down in this case and reprising the fortune it brought in the judicial history by taking in arms 'privacy' as part of our Fundamental Right, it is not possible to deny the criticism it holds in not addressing other legal issues like data privacy and data mining. Will it take another couple of years to address issues of data privacy, sensitive personal information, and data mining as part of the same privacy issue? The only privacy issue addressed in this case was regarding the use of Aadhar Card for availing the basic human needs, like availing of a new SIM card and new LPG connections. The other issues mentioned above were not touched at all. Prior to the *Puttaswamy case* privacy was read under different umbrellas of constitutions like liberty and dignity but nowhere had it talked about the other crucial legal issues attached to privacy. Having said that, now privacy issues as a right is answered and finds its place under article 21.

Privacy law is considered to be consisting of two elements. They are:-

- Firstly, a definition of the circumstances in which third parties have the right to collect, use ,and disseminate personal information about others and
- Secondly, a mechanism for preventing collection, use and dissemination outside those limits.

The first of these is largely culturally determined, with nation- states taking very different views of how information should be treated as private. The second also reflects cultural differences and the national view as to what role the state should play in protecting it as a right.<sup>31</sup> Going back to the history dated 1980, it is to be noted that

---

<sup>31</sup>Chris Reed, *Internet Law* 262-263 (Universal Law Publishing, Co. Pvt. Ltd) (2<sup>nd</sup> Edn.) (2010).

threat to privacy was recognized by two Boston attorneys in the article captioned “The Right of Privacy”, published in the Harvard Law Review.<sup>32</sup>

In India, the Supreme Court under Article 21 attempted time and again to cover the term ‘privacy’ in several cases, *supra* chapter 1. Despite of the laws like Information Technology Act (Act 21 of 2000) 2000 which provides for legal recognition of business conducted over the internet, with numerous sections providing for the protection, as well as punishment in case of failure and omission in respect of e-Commerce activities, the thinkers, research scholars and people at large are overburdened with the issues about privacy, data protection, data mining, validity of e-contracts, etc. in the internet world .Several amendments have modified as well as have included new or additional sections to provide a comprehensive law governing e-Commerce , but it has miserably failed to give a precise and universally accepted definition of the term privacy, data privacy and Sensitive personal information under the Information Technology (Amended) Act, 2008.

Privacy of a person both in offline or online are infringed by many factors,<sup>33</sup> and includes activities which are held to be of illegal nature. Technology has affected personal privacy along with personal data and is repeatedly influencing our understanding of the notion of privacy.<sup>34</sup> The concept of privacy differs from person to person and by considering the taxonomy of privacy with numerous forms, we could get through the haziness surrounding the concept of ‘privacy’.

---

<sup>32</sup>Roger L. Sadler, *Electronic Media Law* 175 (Sage Publications, Inc.) (2005).

<sup>33</sup>Justice Yatindra Singh, *Cyber Laws* 117 (Universal Law Publishing Co. Pvt. Ltd.) (2008).

<sup>34</sup> Rahul Matthan, *Privacy 3.0 Unlocking Our Data-Driven Future* 15 (HarperCollins Publisher)(2018).

## 2.2. Origin and Development of Privacy

“An initial problem with the study of privacy law is the concept of privacy itself”.<sup>35</sup> Privacy is simply a concept of ‘right to be left alone’ and to enjoy a personal space free from interference and scrutiny.<sup>36</sup> One of the most important developments attained by human beings is the creation of the internet. The Most important impact has been on the transmission of information. As there exist multiplayer’s in the locale of the internet, it is, sometimes described as the ‘information technology communications anarchy’<sup>37</sup>.

Privacy is also defined as the right to selective disclosure and one person’s loss of privacy is another’s gain in intimacy<sup>38</sup>. Many scholars are of the view that the onus of proving the right to privacy falls under those who object it.<sup>39</sup> Privacy also forms part of personal liberty and is a prerequisite for an individual to exercise personal liberty and similarly privacy is also an essential feature for a dignified life. The trio of liberty, dignity, and privacy is said to form an integral core of an individual’s existence.<sup>40</sup> Legal protection for privacy existed in western countries too for hundreds of years<sup>41</sup> and so it did in India. In view of Justice Sanjay Kishan Kaul (Judge of

---

<sup>35</sup> Ramesh Kumar, Right to privacy, Ph.D. Thesis, University of Allahabad (2010), available at file:///C:/Users/LIBRARY/Desktop/privacy.pdf (Last visited on November 14, 2019).

<sup>36</sup> Rehana Parveen, *Protection of Privacy in India: Law and Juridical Concerns* (2010), available at [http://shodhganga.inflibnet.ac.in/bitstream/10603/52364/1/01\\_title.pdf](http://shodhganga.inflibnet.ac.in/bitstream/10603/52364/1/01_title.pdf) (Last visited on October 1, 2018).

<sup>37</sup> Kavita, *Copyright in the Digital Age: Internet Issue* (2015), available at [http://shodhganga.inflibnet.ac.in/bitstream/10603/100920/1/01\\_title.pdf](http://shodhganga.inflibnet.ac.in/bitstream/10603/100920/1/01_title.pdf) (Last visited on October 1, 2018).

<sup>38</sup> Gavin Phillipson and Heklen Fenwick “Breach of Confidence as a Privacy Remedy in the Human Rights Act Era” *Modern Law Review* (p. 662) (2000) (Vol.63) (No.1) (Jan-Nov.) (Published for the Modern Law Review limited by publishers).

<sup>39</sup> *Id.*

<sup>40</sup> Abhinav Gupta, *Privacy: Whether a Fundamental Right?* 14 (Prof (Dr.) R. Venkata Rao & Prof (Dr.) T.V. Subba Rao (eds.) “A Public Discourse on Privacy-An Analysis of Justice K.S. Puttaswami v Union of India” (2018).

<sup>41</sup> Raman Mittal & Neelotpal Deka, “Cyber Privacy”, 199 “Legal Dimensions of Cyberspace” (S.K. Verma & Raman Mittal, Eds.), (ILI, Delhi).

Supreme Court), privacy is a fundamental right that guards the individual against intrusion from outsiders and helps in leading an independent life.<sup>42</sup>

Even though it is not at all easy to define the term ‘privacy’, many attempts have been made to give a well-defined concept to the term. Advocates of privacy like<sup>43</sup> Justice Louis Brandeis<sup>44</sup> and Alan F. Westin<sup>45</sup> spoke about the concept of privacy as a desire to be alone and about having control over one’s information and desire to share it only to the extent one wishes to without any compulsion. The concept of privacy also holds a place in the Preamble of the Australian Privacy Charter which states that the right to privacy is an integral part of human beings. They have the right to cut themselves out from the scrutiny of other people. Even though human beings are inevitable in a society, right from interference must be evitable. Such right of seclusion must be respected by the state as well as by private organizations.<sup>46</sup> And now it is prima facie that almost all the Constitution in the world had made an attempt to provide a place for privacy rights of an individual and aimed at protecting the same against intruders. The Right to privacy is debated to be a fundamental right by many western countries and countries like India too had in the past denied it to be a fundamental right and deprived it of constitutional recognition in many former cases before Aadhaar happened.<sup>47</sup>

---

<sup>42</sup>*S. Puttaswami (Retd.) and Ors. v. Union of India and Ors* (2017)10 SCC 1

<sup>43</sup> Raman Mittal and Neelotpal Deka, *Cyber Privacy* 198.

<sup>44</sup> Former American Lawyer and one of the writers of the famous article “The Right to Privacy” published in 4 Harvard L.R.193, 1890.

<sup>45</sup> Author of the Book “Privacy and Freedom”, and one of the most prominent scholars of privacy.

<sup>46</sup> Raman Mittal and Neelotpal Deka, “*Cyber Privacy* 198.

<sup>47</sup>*Supra* Note at 52.

### **2.3. The Legal Issues of Privacy and Data Protection in e-Commerce**

The term legal and techno-legal are not synonymous but have to be read together as they form an important part in e-Commerce when examined in the light of privacy and data protection. The legal issues of privacy and data protection in e-Commerce have been divided under two categories. The first one deals with the lack of definition of these terms under the Indian Statutes/Laws. The second one deals with the issues in these Acts to address problems of privacy and data protection in e-Commerce ecosystem.

#### **2.3.1. Privacy under Indian Laws**

The term privacy has not been defined under any law but still, it is regarded as one of the most important issue in this internet age. In the absence of any legal definition of this term, it becomes really difficult to protect the same especially in e-Commerce. The growth in online transaction with multiple sellers and buyers from different jurisdiction has raised the concern for misuse of data too. With the innovation in technology, the concerns for privacy and data have been felt by many countries including our country, India. It is true that no statutes in India have defined the term privacy but have made an attempt to punish the wrongdoer in events of its violation. The confusion is regarding the provisions of the Information Technology Act, which at the one hand nowhere defines this term but at the other hand provides for a penalty in case of its intrusion. There are grey areas in Indian Laws, when it comes to providing or lacking a definition of the term 'privacy'. The term privacy has many contours and includes terms like, Territorial Privacy, Online Privacy, Data privacy or Information Privacy. These terms have been discussed below in the sub-heading titled '*legal issues in defining privacy*' to understand these terms as well as to realize the

need for having a standard legal definition of the term ‘privacy’ and as well as to be aware of the fact that even though the concept the privacy differs from person to person and among countries in general, but there is an urgency to have one single standard definition to address this issues at both national and international level.

### **2.3.1.1. The Constitution of India**

Right to privacy has been delicately carved by the courts by a creative interpretation of the Article 19 (1) (a) and 21 of the Indian Constitution and after a close analysis of the development of privacy laws in India, it is established that this law evolved basically from torts and Constitution.<sup>48</sup> Though both the law sought to protect privacy they do differ in their approaches in protecting the same. Damages for violating one’s private space are found in common law and reasonable restriction for the intrusion of the same comes under Article 21.<sup>49</sup> No doubt the right to privacy has been recognized and accepted worldwide as an essential human right and it is trite modern law that privacy is an important component of human personality. Human rights are codified in international law through international and regional conventions. Privacy finds a prominent place in each of these regimes. The growth of Indian law has often been guided by international conventions to which India is a signatory. Therefore, these principles occupy an important place in the evolution of rights in India.<sup>50</sup>

Privacy is also termed a fundamental human right. Looking back to history it has been evident that an immense effort has been put on to advance laws on privacy and still there is no such comprehensive law to deal with the legal, techno-legal and regulatory

---

<sup>48</sup> Raman Mittal and Neelotpal Deka, “*Cyber Privacy* 198 “Legal Dimensions of Cyberspace” (S.K. Verma & Raman Mittal, Eds.), (ILI, India).

<sup>49</sup> *Id.*

<sup>50</sup> Rishika Taneja and Sidhant Kumar, *Privacy Law* 7.

issues of protecting privacy and data privacy in e-Commerce <sup>51</sup> . Indian Constitution did not explicitly assured the right to privacy in the past however through various judgments over the years the Judges of the Nation have interpreted other rights in the Constitution to be giving rise to a right to privacy-primarily through Article 21- the right to life and liberty. <sup>52</sup> Different genres of privacy from time have witnessed and been decided by the Apex court of India in different case laws. Earlier right to privacy was not directly considered to be one of the Fundamental Rights. One such instance can be drawn from the case of *Kharak Singh* Supra, where it only laid down that it forms an essential ingredient of Article 21.<sup>53</sup> *R. Rajagopal v State of Tamil Nadu*<sup>54</sup> is another case where it has been stated by the Supreme Court that right to privacy falls under the purview of Article 21 and there is a nexus between Article 19 (1) (a) and 21 which guarantees privacy in one or the other. Further, the Apex Court focused on the concept of seclusion, where one ought to have control over one's information about marriage, pregnancy, family, education, etc. And the publication of such information without prior consent and knowledge would constitute a violation of privacy as indirectly been guaranteed under Article 19 (1) (a) and 21. <sup>55</sup>

Regarding the relevance of International Privacy jurisprudence in India in *Vishaka v. State of Rajasthan*<sup>56</sup>, the position was established that the fundamental rights in the absence of domestic legislation on the subject must be interpreted in line with the

---

<sup>51</sup> Raman Mittal and Neelotpal Deka, *Cyber Privacy* 199 "Legal Dimensions of Cyberspace" (S.K. Verma & Raman Mittal, Eds.), (ILI).

<sup>52</sup>The Right to Privacy in India, (2016), available at [https://privacyinternational.org/sites/default/files/UPR27\\_india.pdf](https://privacyinternational.org/sites/default/files/UPR27_india.pdf) (Last visited on June 22, 2017).

<sup>53</sup>*Kharak Singh v. State of Uttar Pradesh, Govind v. State of Madhya Pradesh, R. Rajagopal v. State of Tamil Nadu, Gobind v. State of M.P., Kharak Singh v State of U.P., Vishaka v. State of Rajasthan, People's Union for Civil Liberties v. Union of India, M.P. v. Satish Chandra.*

<sup>54</sup> AIR 264, 1994 SCC (6) 632

<sup>55</sup>Right to Privacy in India, available at <http://www.indialawjournal.org/archives/volume7/issue-2/article3.html> (Last visited on July 22, 2017).

<sup>56</sup> AIR 1997 SC 3011



provisions of international treaties and conventions to which India is a party. The position is that international legal instruments are an important part of municipal jurisprudence in India. The principles of international human rights law provide significant direction to domestic law as well. Therefore, determinations based on these instruments can serve as the basis of the growth of privacy law in India. The Supreme Court while dealing with the first case concerning privacy did accord recognition to privacy as a human right. However, the majority did not elevate privacy to constitutional status.<sup>57</sup> The same approach was undertaken by the court in *Gobind v. State of M.P.*<sup>58</sup>. It cited with approval from *Kharak Singh v State of U.P.*,<sup>59</sup> the rulings addressing the favor for a qualified right to privacy. The Supreme Court of India undertook a detailed consideration of privacy as a right in *R. Rajagopal v. State of T.N.*<sup>60</sup> and accepted that “right to be let alone” falls under the ambit of Article 21 whilst citing privacy as a prominent human right concern. Provisions of ECHR and ICCPR also confirmed to strengthen the contention that privacy is one of the basic human rights. This right is not contrary to municipal law and is rightly interpreted from the phraseology of Article 21.<sup>61</sup> The principles contained in the ECHR, UDHR and the ICCPR are, therefore, by the law declared by the Supreme Court are parts of the Indian law on privacy.<sup>62</sup>

Human Rights law guards the ‘right to privacy’ of every individual irrespective of where they belong. Due to the effort of this Law ‘right to privacy’ has been recognized as one of the most essential rights of human beings. In India, though this

---

<sup>57</sup> *Kharak Singh v State of U.P.*, AIR 1963 SC 1295: (1964) I SCR 332

<sup>58</sup> (1975)2 SCC 148:1975 SCC (Cri) 568: AIR 1975 SC 1378

<sup>59</sup> AIR 1963 SC 1295: (1964) I SCR 332

<sup>60</sup> (1994) 6 SCC 632: AIR 1995 SC 264

<sup>61</sup> Rishika Taneja and Sidhant Kumar, *Privacy law Principles, Injunctions and Compensation* 10-11 (2014).

<sup>62</sup> Raman Mittal and Neelotpal Deka, *Cyber Privacy* 199.

right was not well recognized and lacked a legal sanction in the form of Bill, it was time and again argued in the Courts. Article 19 (1) (a) and Article 21 are the pillars under our Constitution that incorporate 'privacy' as one of the basic fundamental rights. There was an issue regarding the protection of individuals 'right to privacy' in the public domain as this right did not go beyond its protection against third parties. The Apex Court accepted the idea of 'private law actions' in the occasion of the bridge of this right and to bridge a gap brought a nexus between the two. Therefore, the violation of privacy can be redressed by civil actions for injunctions and damages. After emerging as a fundamental right, the right to privacy has undergone a process of evolution. The ambit of this right now covers most areas of human life and personality viz; bodily privacy, sexual relations, women's rights among other important human rights concerns.<sup>63</sup>

The province of privacy of an individual came to be determined by law. In the first claim for a right to privacy, the Supreme Court declined to impute a constitutional element of privacy in *M.P. v. Satish Chandra* supra. The right to privacy has acquired the legal sanctity of a fundamental right. However, it is essential to keep in mind that barring a few exceptions, fundamental rights secured to the individual are limited only by State action. Thus, such an interpretation will not protect an individual against the actions of private parties, as enunciated in *P.D. Shamdasani v. Central Bank of India Ltd.*<sup>64</sup> . The Supreme Court in *Auto Shanker case*<sup>65</sup> recognized privacy as a right that is capable of claiming damages<sup>66</sup> when encroached without consent and knowledge<sup>67</sup> .

---

<sup>63</sup>*Supra* Note at 67.

<sup>64</sup> AIR 1952 SC 59:1952 SCR 597

<sup>65</sup> (1994) 6SCC 632

<sup>66</sup>Rishika Taneja and Sidhant Kumar, *Privacy Law, Principles, Injunctions and Compensation* (2014).

<sup>67</sup>*Id.*

### 2.3.1.1.1. Legal issues in defining Privacy

The Government can protect its Citizen's 'privacy', if she wishes to.<sup>68</sup> 'Privacy' is not at all easy to define.<sup>69</sup> In a contemporary virtual era, privacy has been recognized both by law and in common parlance. But it varies in different legal systems as they emphasize different aspects.<sup>70</sup> The conceptualization of privacy and right to privacy is not so easy. It differs in numerous ways depending on different situation.<sup>71</sup> The difficulty is that of the legal nature faced by the e-Users. The issue is not limited to Indian jurisdiction but has a global reach by virtue of 'Cloud Computing'<sup>72</sup>. The term 'privacy' has been described as individuals desire to have control on the distribution of his/her information to the world.<sup>73</sup> Some authors are of the view that privacy is a choice of each individual's not to communicate.<sup>74</sup> Previously right to privacy was available to a person only with respect to his property, now after the judicial victory brought in the case of *Puttaswami supra* privacy has gained prominence in the fundamental rights enshrined in the Constitution of India.<sup>75</sup> And now it is available to an individual against the State.<sup>76</sup> Even after this victorious pronouncement by the Supreme Court, the legal issues indebted with that of vague definition of the term 'privacy' remains unsettled. With a sweeping swing in the cyber network and threat of being interrupted and fear of losing control over personal information in the platform

---

<sup>68</sup>*Tulane Law Review* 1219 (May 1994).

<sup>69</sup>The notion of privacy varies from person to person and from country to country. Protection of privacy is a mode of drawing a limit on how far a society can intrude into a person's affairs, *available at* <https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/> (Last visited on July 23, 2018).

<sup>70</sup> Shiv Shankar Singh, "Privacy and Data Protection in India: A Critical Assessment", (Vol. 53, 1-4, 2011) *JL of the Indian Law Institute*, 664), 53 *JILI*, 2011.

<sup>71</sup>*Id.*

<sup>72</sup> As clouds in the sky keeps on moving from one place to another, movement of cloud computing in a similar way are not fixed and static and moves from one place to another providing services. It is not only for storing of data. It is more than that as it provides services. For easy management of data, companies often hire Cloud service providers to do the needful and pay accordingly, *available at* <https://azure.microsoft.com/en-in/overview/what-is-cloud-computing/> (Last visited on July 23, 2018).

<sup>73</sup>S.K. Verma and Raman Mittal (eds.) *Legal Dimensions of Cyberspaces*, 98 (ILI, Delhi).

<sup>74</sup>*Supra* Note at 59.

<sup>75</sup>*Olmstead v Unites States* (1928)

<sup>76</sup>S.K. Verma and Raman Mittal (eds.), *Legal Dimensions of Cyberspaces* 198 (ILI, Delhi).

of virtual world, the need for privacy and its recognition came in the forefront. Privacy is a right which is so vital that every individual would expect it to be protected.<sup>77</sup> Having a standard definition of ‘privacy’ will not only help in resolving the legal issue it carries with itself but will also help in underpinning the relief in the event of intrusion.

Intrusion into people’s life is not new. People were under scrutiny even back in the years when technology was an alien to the society and digital network was an unheard threat. Privacy tort law is one the product of the prior era’s hazard.<sup>78</sup> Snap cameras and recording devices were a means to capture private moments of the people without detection back in the 19<sup>th</sup> centuries. This is to say that people were under scrutiny even when there was no technological innovation and with the advancement of technology this has gained a momentum and privacy of individuals are under grave menace. Back then press used to gain profit from selling peoples gossips, their private photographs without their consent, in short privacy was not considered as an important aspect of people’s life.

The birth of Tort Privacy owes to the two prominent scholars, Samuel Warren and Louis Brandels. In 1890’s they advocated ‘privacy’ to be an integral part in protecting person’s right in the development of his personality free from unwanted publicity and unwanted access by others. Almost after 70 years Privacy Tort was restructured by

---

<sup>77</sup> It is weird that in this technological driven era one has to cry for the protection of their privacy and personal information’s upon which nobody has the right to intrude into. Why do an individual needs to be so scared of their privacy and information? It is really frustrating to know that our rights are under scrutiny and under threat of being misused by third person for immoral gains and the laws are too deaf and blind to address such nuisance. Internet should be helping the people and make their work easy and should not terrorise the customers who are engaged in e-Commerce, Jathan Sadowski (Feb. 26. 2013), Why does Privacy Matter? One Scholar’s Answer, *available at* <https://www.theatlantic.com/technology/archive/2013/02/why-does-privacy-matter-one-scholars-answer/273521/> (Last visited on July 23, 2018).

<sup>78</sup>Danielle Keats Citron, *Mainstreaming Privacy Torts* 1807.

William Prosser and conceived it under four wrongs. For him privacy tort law protected an individual against emotional, reputational and proprietary injuries caused by (1) public disclosure of private facts, (2) intrusion on seclusion, (3) depiction of another in a false light, and (4) appropriation of another's image for commercial gain.<sup>79</sup> Even though Prosser modern tort law served courts with blended theory and practice of redressing harm it failed to take into purview the essence of interest of privacy that tort law intends to protect and thus narrowed the person's right to develop his personality as opined by Samuel Warren and Louis Brandeis.

Scholars like Danielle Keats Citron analyzed William Prosser's restatement of tort laws on protection of the "right to privacy" and concluded it to be inadequate, narrow and rigid in conceptualizing privacy interest implicated by networked technologies.

Though both the eras depicted privacy invasion to have caused psychic and reputational wounds of a specific genus, Courts asserted on having a proof of those alleged injuries as those injuries were ethereal in nature and of much trivialities.<sup>80</sup>

Regrettably privacy tort law fails short in addressing the present threat to privacy. During the nineties intrusion of privacy of an individual was traded only through newspapers which remained in circulation for only a couple of days, later ending up in a library files, this is to say that the audience soon forgot the news and it was not easily accessible for an indefinite period as it is today. Considering today's scenario, intrusion of privacy has been magnified to a larger audience that too for an indefinite time and easily available unaffected by the territory of the viewer. Today information is available at just a click. Cloud computing has become the parent in triggering the sensitive personal information, information/ data of a group and of an individual

---

<sup>79</sup>*Supra* Note at 71.

<sup>80</sup>*Id.*

under a larger scrutiny and at larger third-party control. Since internet is permanent in nature and easily searchable, privacy of people is under extreme threat and exacerbates individual's emotional and reputational injuries. The worse of the worse is the issue of 'Data Theft' which encourages the third parties to assault individuals not even being traceable, which intensifies mental and reputational injuries. There has been change in the facet of privacy injuries with much wider dimension. To quote some chronological transformation, in the nineties privacy intrusion only inflicted psychic and reputational harm<sup>81</sup> but with the advancement in technology and digital network the taxonomy of privacy intrusion has reached another phase.

Prosser's tort law revolved around tort injuries caused by hazards, to say he had a limited approach towards privacy protection of an individual and emphasized more on the harms caused by privacy intrusion. This harm based approach was exemplified by Oliver Wendell Holmes, he explained that 'the evil against which tort law was directed was the inflicting of harm and tort law protected against harms and remedied them not because they were wrong but because they were harms'<sup>82</sup> , Whereas G. Edward White described Prosser's methodology as "Consensus Thought".<sup>83</sup> Anita Bernstein on the other hand agreed on crucial role of Prosser's blend of doctrine and policymaking in the success of his privacy taxonomy. Despite of his reign in tort law, and a pragmatic approach towards twentieth century privacy intrusion, many contemporary privacy injuries is left uncompensated.<sup>84</sup>

---

<sup>81</sup>*House v Pith*, (1956)

<sup>82</sup>Danielle Keats Citron, *Mainstreaming Privacy Torts* (1822).

<sup>83</sup>*Supra* Note at 86.

<sup>84</sup>*Id.*

As the definition of privacy varies from person to person it is not easy to describe privacy under a glass ceiling. With the advancement in technology the concept of privacy is changing and is not limited to the word 'privacy' only. The undeniable domains of privacy and data are guiding in finding and knowing the harm and associated problems in protecting the same.<sup>85</sup>

The distinguished domains of 'privacy' and 'data' will aid to have an insight into the ongoing issues of privacy and data protection in the perils of e-Commerce. The concept of Information Privacy<sup>86</sup> or Personal Data has always been a topic of discussion. Privacy as a distinct subject has not been defined under any statutes but different types of privacy have been defined, they are as follows:

2.3.1.1.1.i. Territorial Privacy: It is a form of privacy that restricts interference in the lives of individual whether it is in office, market or open space. Genetic Privacy mainly refers to the right which is related to personal information relating to private life of an individual on which one will have full control against any third party.<sup>87</sup>

---

<sup>85</sup> *Supra* Note at 84.

<sup>86</sup> Information Privacy means the protection which includes both control and right over personal information. It further includes liberty of keeping the information with oneself and its distribution to other entities. Some argues that this right over one's information is not absolute and is vulnerable to intrusion. Whenever there is an online privacy issue, there is involvement of at least two parties viz., the data subject and the collector. Collectors are often referred as searchers. Personal records and private data are also a part of Information Privacy. It is one of the most important parts of the whole gamut of the concept of privacy. According to Wikipedia Information Privacy/ Data Privacy (or Data Protection) involves collection and dissemination of the collected data. And the challenge lies in bringing up a balance between utilization of those collected data and protection of data subjects. Since laws relating to Privacy and Data protection is unstable and because India does not have Laws of Data protection it becomes important to keep updated with the unstable law, *available at* [https://www.researchgate.net/publication/259502676\\_State\\_of\\_the\\_Information\\_Privacy\\_Literature\\_Where\\_are\\_We\\_Now\\_And\\_Where\\_Should\\_We\\_Go](https://www.researchgate.net/publication/259502676_State_of_the_Information_Privacy_Literature_Where_are_We_Now_And_Where_Should_We_Go) (Last visited on July 23, 2018).

<sup>87</sup> *Genetic Privacy, available at* <https://en.wikipedia.org/w/index.php?search=Genetic+privacy&title=Special:Search&profile=default&fulltext=1&searchToken=51ecq6ozrmlbw3mg6i103jj1r> (Last visited on July 23, 2018).

2.3.1.1.1.ii. Online Privacy: When it comes to Online Privacy, it's not an easy subject in a country like India. Cyber space privacy of personal information refers to the right of the data subjects to enjoy the peace in the network's private life along with its protection in accordance with law. It should not be infringed, known, collected, copied, disclosed or utilized without the free consent of the data subject. Internet Privacy/Online Privacy & Cyber Privacy is often used interchangeably. It includes the main elements: personal data, private information, and individual field.<sup>88</sup> It refers to the security level of personal data available in the internet. It comprises of variety of factors, techniques and technologies which is used in protecting sensitive and private data, communications and preferences.<sup>89</sup> Hijacking, spyware and adware are some examples of Privacy-invasive software that overlook user's privacy and are circulated with a commercial intention.<sup>90</sup>

2.3.1.1.1.iii. 'Data Privacy' or 'Information Privacy': According to Wikipedia 'Data Privacy' or 'Information Privacy' is the collection and dissemination of data.<sup>91</sup>

### **2.3.1.2. Indian Laws on Privacy and Data Protection**

The lack of definition of the term privacy and data privacy in Indian laws is the most crucial legal issues so far. There are laws in India which deals with e-Commerce, e-Contract, digital signatures etc. but nowhere these laws have defined the above stated

---

<sup>88</sup> Sumeet Kumar Singh, "Spamming: Is It Infringement of Privacy" (p. 28) (January- March) (2011 Cri LJ 1) [All India Reporter (Pvt. Ltd)].

<sup>89</sup> The Amendments brought in 2011 in the I.T. Act requires an organisations processing personal information to get permission from the owner of data in writing, *available at* <https://www.google.com/search?q=2011+amendment+act+of+I.T.+Act&oq=2011+amendment+act+of+I.T.+Act&aqs=chrome.69i57j33.12322j0j7&sourceid=chrome&ie=UTF-8> (Last visited on July 23, 2018).

<sup>90</sup> Privacy Invasive, *available at* [https://en.wikipedia.org/wiki/Privacy-invasive\\_software](https://en.wikipedia.org/wiki/Privacy-invasive_software) (last visited on July 23, 2018).

<sup>91</sup> Data Privacy, *available at* <https://en.wikipedia.org/w/index.php?search=Data+privacy&title=Special:Search&profile=default&fulltext=1&searchToken=7r2p9ktjwll6izasy5225ec86> (Last visited on July 23, 2018).



terms. The lack of legal definition makes it difficult to make the loss good in events of its infringement in an online environment where e-Commerce happens beyond borders and untraceable jurisdictions. Information Technology Act, 2000 and Information Technology (Amended) Act, 2008 are the parent and most important Acts in India which was formulated on UNCITRAL Model Laws to give legal validation to e-contracts and digital signatures to facilitate e-Commerce. Apart from these two Acts, SEBI, Consumers Protection Acts, Indian Contract Acts, Indian Penal Code as well as R.B.I. guidelines indirectly and sub-consciously touches the parameters of the two crucial legal issues of privacy and data protection in India.

Despite of having numbers of above mentioned laws, none of them are effective to cope up and handle the menace of technology and stop their interference in personal space and data of individual while enjoying the benefits offered by the technology in this contemporary era.

#### **2.3.1.2.1. Information Technology Act, 2000 (Act 21 of 2000)**

Information Technology Act is the most piece of legislation and is commonly known as the I.T. Act of 2000. It too had some objectives which can be precisely divided into three parts. E-Commerce is one specific area of this Act following the footsteps of UNCITRAL Model Law. The first was to provide legal recognition to e-Commerce transactions, second was filing of documents with government agencies through electronic medium, and third was to amend certain laws. Other important features include legal validation to e-contracts and recognition of electronic documents.<sup>92</sup> Originally the Act contained 94 sections, 13 chapters and 4 schedules. This Act is applicable to

---

<sup>92</sup> S. Praveen Raj and Aswathy, "Comparison between Information Technology Act, 2000 & 2008", *International Journal of Pure and Applied Mathematics* (Volume 119 No. 17 2018, 1741-1756), available at <https://acadpubl.eu/hub/2018-119-17/2/141.pdf> (Last visited on January 16, 2019).

every Indian States. A person shall be punished under this Act if he commits a crime by using a computer based in the Indian Territory. The preamble of this Act states “*it shall extend to the whole of India*”.<sup>93</sup> The applicability of this Act is not only limited within India but extends to other nationalities too “*if any offence is committed by a person outside India*”.<sup>94</sup> In order to keep tandem with the new technologies, certain sections of the other Indian Statutes were also amended by this Act.<sup>95</sup>

Information Technology is the creation of internet and e-Commerce is the best type of commerce so facilitated. During, the last couple of years, e-Commerce has become a very important part of our lives and it basically revolves around computers, internet and cyberspace. We all are aware of the modern issues of internet but hardly few of us know what does it mean, so in order to understand the term ‘internet’ and ‘cyberspace’ let us have a look into the case of *ACLU v Reno*<sup>96</sup>, where the term ‘internet’ and its development have been explained by the District Court for the Eastern District of Pennsylvania in the following words:

*“The internet is not a physical or tangible entity, but rather a giant network, which interconnects innumerable smaller groups of linked computer networks. It is thus a network of networks”*.<sup>97</sup>

In the similar case of *ACLU v Reno supra*, the U.S. Court has explained the nature of ‘Cyberspace’ as:

---

<sup>93</sup> Section 1(2), Information Technology Act, 2000

<sup>94</sup>*Id.*

<sup>95</sup>Indian Penal Code, 1860, Indian Evidence Act, 1872, Banker’s Book Evidence Act, 1891, and Reserve Bank of India Act, 1934.

<sup>96</sup>521 US 844

<sup>97</sup> Justice Yatindra Singh, *Cyber Laws* 3- 4, (Universal Law Publishing Co. Pvt. Ltd) (2007).

“Anyone with access to the internet may take advantage of a wide variety of communication and information retrieval methods. These methods are constantly evolving and difficult to categorise precisely. But, as presently constituted, those most relevant to this case are electronic mail (“e-mail”), automatic mailing services (“mail exploders, “sometimes referred to as “listservs”), “newsgroups”, “chat rooms”, and the “world wide web”. All of these methods can be used to transmit text; most can transmit sound, pictures, and moving video images. Taken together, these tools constitute a unique medium known to users as “cyberspace”-located in no particular geographical location but available to anyone, anywhere in the world, with access to the internet”.<sup>98</sup>

#### **2.3.1.2.2. Information Technology (Amendment) Act, 2008**

The Parent Act of 2000 had concentrated on promoting I.T. industry, regulation of e-Commerce, e-Governance and prevention of cybercrimes. The Act failed to address new offences of cyber crimes and therefore a need for the amendments in the Information Technology Act, 2000 was felt. In order to insert new offences of cyber crimes an amendment in the year 2008 was passed by the Parliament and was made effective from 27<sup>th</sup> October, 2009. The Information Technology Amendment Act, 2008 is the extension of the Information Technology Act, 2000. Certain remarkable changes were brought by the amendments which included modification in the term “communication device” for incorporating terms like, current use, validation of

---

<sup>98</sup>*Supra* Note at 94.

electronic signatures and contracts to make the original owner of IP address responsible for content accessed and distributed.<sup>99</sup>

The issue in the Act of 2000 and 2008 is nowhere the term privacy and data privacy has been defined. Punishment for violation of privacy is provided U/S 66 E<sup>100</sup> of the Information Technology Act, 2008.<sup>101</sup>

This section is vague and incompetent in this technological era where the concept of privacy is very huge and threatened on a day to day basis with the use of computers and internet. This term cannot be confined only to private area of a person. In this technologically driven era, privacy includes whole lot of other things and needs to be protected under any form. The Supreme Court of India recognized the right to privacy a fundamental right guaranteed under very important provision of Constitution of India, article 21 and now it's time to include it under the Information Technology Act, 2008 too. Inclusion of this term along with data privacy would widen the nature and scope and will help in modifying or amending section 66E in the light of this new cybercrime phase.

### **2.3.1.2.3. The Indian Contract Act, 1872 (No.9 Act of Parliament)**

Contract in virtual world differs from the one that takes place in a physical market. In e-Commerce the issue is that of forming a valid and legally binding e-Contract. The

---

<sup>99</sup> S. Praveen Raj & Aswathy, "Comparison between Information Technology Act, 2000 & 2008", *International Journal of Pure and Applied Mathematics*, (Volume 119 No. 17 2018, 1741-1756), available at <https://acadpubl.eu/hub/2018-119-17/2/141.pdf> (Last visited on January 16, 2019).

<sup>100</sup> Section 66 E. Punishment for violation of Privacy (Inserted vide ITA, 2008).- Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both

<sup>101</sup> Section 66E, The Information Technology (Amendment) Act, 2008.

most often asked question is “How e-contracts can be formed, performed and enforced as parties replace paper documents with e-media”.<sup>102</sup> Even though the Information Technology Act, 2000 deals with contractual aspects like use of electronic records, such as attribution, acknowledgement, time and place of dispatch and receipt, it has to be read with the Indian Contract Act, 1872 because the former act is only an enabling act.<sup>103</sup> The issue here is there is no direct communication between the sender and receiver in online platform and message sent via e-mail breakdown while travelling through the internet leading to issues of exact time of communication of acceptance of the contract.

The main elements of contract under the Indian Contract Act are offer, acceptance and consideration for the contract. These same elements are required in e-contract but the issues here is that of online identity. There is no pre-existing relationship between the contracting parties in e-Commerce transaction and raises issues like person’s identity, capacity and legitimacy to enter the contract. To identify a person in e-contract I.T. Act, 2000 introduced ‘Digital Signature’ as a method to identify person’s identity in virtual market. I.T. Act also provide legal recognition to e-contracts, by providing a method to determine the exact time and place of dispatch and receipt of the e-mail.

A contract is considered to be a contract only if it fulfills the parlance of Section 2(h) of the Indian Contract Act.<sup>104</sup> Section 2 (c) states that on acceptance of the offered

---

<sup>102</sup> K. Susheel Barath & Dr. V. Mahalakshmi, “Legal Issues in e-commerce transactions –An Indian Perspective”, 185, (Volume 4, Issue 11,) (International Journal on Recent and Innovation Trends in Computing and Communication), *available at* <https://ijritcc.org/index.php/ijritcc> (Last visited on December 13, 2020).

<sup>103</sup>*Id.*

<sup>104</sup> Section 2 (h), Indian Contract Act, 1872

proposal it becomes a promise and binds the persons to contract by way of conferring legal rights and obligations. The Indian Contract Act also incorporates the *doctrine of privity of contract*,<sup>105</sup> which clearly states that the contract only binds the people who are party to it and excludes third party, and only bonafide parties have the right to sue the other party in a contract. The doctrine of Privity, third party, rights and obligations of parties in a contract have been discussed by the Supreme Court in *K.P.M. Builders Private Limited v. National Highways Authority of India and Another*.<sup>106</sup> In this case the Supreme Court opined that third party, who is not a party to contract, is not entitled at all to seek remedy.

The issue of privity of contract exists both in traditional and virtual world but addressing this issue is much simpler in traditional contract as parties to a contract comes face to face and it is easier to identify the same. The issue is complex in a virtual world as it is very difficult to prove the relationship of agency between the parties to contract.<sup>107</sup> In an online contract apart from the buyer and seller, a number of hosting websites are involved and multiplicity of players in online business invites many issues in contract like, rights and liabilities of third parties.

#### **2.3.1.2.4. The Securities and Exchange Board of India Act, 1992 (15 of 1992), (SEBI)**

SEBI Act came in the year 1988, to promote healthy expansion of the securities market and for the protection of investor's. This Act came into force on January 30, 1992. Activities like stock exchange, mutual funds, merchant bankers, etc. were

---

<sup>105</sup> Privity of Contract, *available at* <http://www.legalservicesindia.com/article/378/Privity-of-contract-&-third-party-beneficiary-in-a-contract.html> (last visited on February 13, 2020).

<sup>106</sup> (2015) 15 SCC 394

<sup>107</sup> Raghavendra S. Srivasta and Sukruta R., "Online Contracts", *available at* <http://14.139.60.114:8080/jspui/bitstream/123456789/722/9/Online%20Contracts.pdf> (Last visited on February 13, 2020).

monitored by this Act and it extends to the whole of India. The Securities and Exchange Board of India Act, 1992 (15 of 1992), have been amended by the Securities and Exchange Board of India (Amendment) Act, 2013 (22 of 2013).<sup>108</sup>

In this internet age, investors are also threatened with the issues of privacy and data protection. And nowhere this Act has defined these terms nor has made any provisions for punishing the wrongdoer.

Securities on internet were not valid in India and no specific provisions were there for the protection of confidentiality and net trading. But, with the passing of the Information Technology Act, 2000 SEBI announced that securities on internet shall be made valid in India. The other lacunas were too removed by this Act of 2000.<sup>109</sup> SEBI now provides policy for seeking data<sup>110</sup>. It aims to facilitate access to data. It has also provided definition of various terms such as Data<sup>111</sup>, Data Custodian<sup>112</sup>, Data Analytics Controller<sup>113</sup>, Data seeker<sup>114</sup>, Data Expunging<sup>115</sup> and Data Anonymization<sup>116</sup>.

---

<sup>108</sup> The Securities and Exchange Board of India Act, 1992 (Universal Law Publishing Co. Pvt. Ltd.) (2014).

<sup>109</sup> S. Praveen Raj & Aswathy, "Comparison between Information Technology Act, 2000 & 2008", *International Journal of Pure and Applied Mathematics*, (Volume 119 No. 17 2018, 1741-1756), available at <https://acadpubl.eu/hub/2018-119-17/2/141.pdf> (Last visited on January 16, 2019).

<sup>110</sup> *Supra* Note at 94.

<sup>111</sup> Securities and Exchange Board of India (SEBI) defines data as information's in structural and unstructured form collected and reported in various databases, Guidelines for seeking Data (2019), available at <https://www.sebi.gov.in/pdf/guidelines-of-data-sharing-final.pdf> (Last visited on February 6, 2020).

<sup>112</sup> In SEBI, Data Custodian is appointed in the internal department for propose of collections, processing and holding of the Data under their custody upon which they exercise their ownership in carrying out the functions related to their department, Guidelines for seeking Data (2019), available at <https://www.sebi.gov.in/pdf/guidelines-of-data-sharing-final.pdf> (Last visited on February 6, 2020).

<sup>113</sup> A team of person who is assigned by Information Technology of SEBI in supervising the activities related to sending data from its deployed officials to interested individual's via media are called Data Analytics Controller, Guidelines for seeking Data (2019), available at <https://www.sebi.gov.in/pdf/guidelines-of-data-sharing-final.pdf> (Last visited on February 6, 2020).

<sup>114</sup> Research activities are carried out by data seeker who are engaged in educational and research institutions, Guidelines for seeking Data (2019), available at <https://www.sebi.gov.in/pdf/guidelines-of-data-sharing-final.pdf> (Last visited on February 6, 2020).

There are no provision for the protection of privacy and data privacy in the SEBI Act, 1992 and in the SEBI (Amendment) Act, 2013 but however according to the reporters of “Business Standard Budget, 2020”<sup>117</sup> privacy and data issues have been undertaken seriously by this Act and ensures investor’s privacy rights on their data.

### 2.3.1.2.5. The Consumer Protection Act, (COPRA) 1986

This Act extends to whole of India and is not binding on Jammu & Kashmir. This Act is the guardian laws which aims for the protection of Consumer’s interest and as such have made provisions for establishment of Councils<sup>118</sup> and other authorities for settlement of disputes according to procedures prescribed by law.<sup>119</sup>Section 2 clause (b) of the Act defines “complainant”<sup>120</sup> and clause (c) defines “complaint”<sup>121</sup> and clause (d) defines “consumer”<sup>122</sup>. This Act was amended in the year 2012, which

---

<sup>115</sup> Removal or deletion of data on fulfillment of the required task is known as data expunging, Guidelines for seeking Data (2019), available at <https://www.sebi.gov.in/pdf/guidelines-of-data-sharing-final.pdf> (Last visited on February 6, 2020).

<sup>116</sup> Identification and sanitization of data is known as data anonymization, Guidelines for seeking Data (2019), available at <https://www.sebi.gov.in/pdf/guidelines-of-data-sharing-final.pdf> (Last visited on February 6, 2020).

<sup>117</sup>Pavan Burugula and Advait Rao Palepu, available at [https://www.business-standard.com/article/markets/sebi-to-come-up-with-special-policy-to-ensure-data-privacy-for-investors-118082600515\\_1.html](https://www.business-standard.com/article/markets/sebi-to-come-up-with-special-policy-to-ensure-data-privacy-for-investors-118082600515_1.html) (Last visited January 18, 2020).

<sup>118</sup> Consumer Protection Act, 1986, (No 68, Acts of Parliament) India: s.4 & 5, Chapter II.

<sup>119</sup>*Id.*

<sup>120</sup>The Consumer Protection Act, 1986, (No 68, Acts of Parliament), .- s. 2 (b.), “complainant” includes.- (i) a consumer; or (ii) any voluntary consumer association registered under the Companies Act, 1956 (1 of 1956) or under any other law for the time being in force; or (iii) the Central Government or any State Government; [(iv) one or more consumers, where there are numerous consumers having the same interest;] who or which makes a complaint;

<sup>121</sup> The Consumer Protection Act, 1986, (No 68, Acts of Parliament) .-s.2 (1) (b) of this Act defines complaint" as issues made in written form. As per this section complainant is regarding any.-

(i) an unfair trade practice or a restrictive trade practice has been adopted by any trader; (ii) the goods bought by him or agreed to be bought by him suffer from one or more defects; (iii) the services hired or availed of or agreed to be hired or availed of by him suffer from deficiency in any respects; (iv) a trader has charged for the goods mentioned in the complaint a price in excess of the price fixed by or under any law for the time being in force or displayed on the goods or any package containing such goods; (v) goods which will be hazardous to life and safety when used, are being offered for sale to the public in contravention of the provisions of any law for the time being in force requiring traders to display information in regard to the contents, manner and effect of use of such goods, with a view to obtaining any relief provided by or under this Act;

<sup>122</sup> The Consumer Protection Act, 1986, (No 68, Acts of Parliament).-s. 2 (1)(d), defines the term "consumer" as any person who.-



inserted and modified various sections<sup>123</sup>. With the passage of time and advancement in technology, new issues of consumer protections have emerged calling for effective and speedy redressal. Thus Consumer Protection Bill, 2018 was introduced in Lok Sabha on 5<sup>th</sup> of January 2018 by the Minister of Consumer Affairs, Food and Public Distribution, Mr. Ram Vilas Paswan. It replaces the Consumer Protection Act, 1986. It introduced provisions relating to product liability and unfair contracts. It also creates a regulatory body called the Central Consumer Protection Council and permits mediation for settlement of consumer complaints<sup>124</sup>.

#### **2.3.1.2.6. The Consumer Protection Act, 2019 (No. 35 of 2019)**

The Consumer Protection Act, 2019 (No. 35 of 2019), received assent of the President on 9<sup>th</sup> of August 2019. This Act extends to whole of the India except the State of Jammu & Kashmir. This Act mainly came with the objectives of protecting interest of the consumers, establishment of authorities for them for timely and effective administration and lastly for settlement of their disputes. The term ‘consumer’<sup>125</sup>,

---

(i) buys any goods for a consideration which has been paid or promised or partly paid and partly promised, or under any system of deferred payment and includes any user of such goods other than the person who buys such goods for consideration paid or promised or partly paid or partly promised, or under any system of deferred payment when such use is made with the approval of such person, but does not include a person who obtains such goods for resale or for any commercial purpose; or (ii) hires or avails any of these services for a consideration which has been paid or promised or partly paid and partly promised, or under any system of deferred payment and includes any beneficiary of such services other than the person who hires these services for consideration paid or promised, or partly paid and partly promised, *Explanation.—*

For the purposes of sub-clause (i), "commercial purpose" does not include use by a consumer of goods bought and used by him exclusively for the purpose of earning his livelihood, by means of self-employment;

<sup>124</sup> Section 4, Supra Note 122

<sup>125</sup> The Consumer Protection Act, 2019, No. 35 of 2019, India, Acts of Parliament, s.7, “consumer” means any person who.—

(i) buys any goods for a consideration which has been paid or promised or partly paid and partly promised, or under any system of deferred payment and includes any user of such goods other than the person who buys such goods for consideration paid or promised or partly paid or partly promised, or under any system of deferred payment, when such use is made with the approval of such person, but does not include a person who obtains such goods for resale or for any commercial purpose; or (ii) hires or avails of any service for a consideration which has been paid or promised or partly paid and partly promised, or under any system of deferred

‘consumer dispute’<sup>126</sup>, ‘consumer rights’<sup>127</sup>, have been defined by this Act under section 7, 8 and 9 respectively. Unlike the Consumer Protection Act of 1986, this Act of 2019 has incorporated the term ‘online transactions’. The parent Act of 1986 had only included six types of unfair trade practices like false representations etc. The new Act has added another three to the list like disclosure of personal information given in confidence etc.<sup>128</sup>E-Commerce is the definition that has positive impact and thus fills the gaps of our old Consumer Protection Act, of 1986 which failed to give a name to this emerging and important term in digital market, thus the most prominent feature of this Act of 2019 is that it has defined the term ‘e-commerce’<sup>129</sup> under section 16.

Before the commencement of this Act of 2019, a bill was proposed in 2018 for its consideration before both the Houses of Parliament, commonly known as the

---

payment and includes any beneficiary of such service other than the person who hires or avails of the services for consideration paid or promised, or partly paid and partly promised, or under any system of deferred payment, when such services are availed of with the approval of the first mentioned person, but does not include a person who avails of such service for any commercial purpose.

*Explanation.*—For the purposes of this clause,—

(a) the expression "commercial purpose" does not include use by a person of goods bought and used by him exclusively for the purpose of earning his livelihood, by means of self-employment; (b) the expressions "buys any goods" and "hires or avails any services" includes offline or online transactions through electronic means or by teleshopping or direct selling or multi-level marketing;

<sup>126</sup> The Consumer Protection Act, 2019, No, 35 of 2019, India, Acts of Parliament, s.8, defines “consumer dispute” as a dispute where the person in question denies or disputes the allegations contained in the complaint;

<sup>127</sup> The Consumer Protection Act, 2019, No, 35 of 2019, India, Acts of Parliament s.9, defines "consumer rights" as.-

(i) the right to be protected against the marketing of goods, products or services which are hazardous to life and property; (ii) the right to be informed about the quality, quantity, potency, purity, standard and price of goods, products or services, as the case may be, so as to protect the consumer against unfair trade practices; (iii) the right to be assured, wherever possible, access to a variety of goods, products or services at competitive prices; (iv) the right to be heard and to be assured that consumer's interests will receive due consideration at appropriate fora; (v) the right to seek redressal against unfair trade practice or restrictive trade practices or unscrupulous exploitation of consumers; and (vi) the right to consumer awareness;

<sup>128</sup>manulawskills, “Difference between Consumer Protection Act, 1986 and Consumer Protection Act, 2019”, *available at* <https://blog.lawskills.in/2019/08/14/differences-between-consumer-protection-act-1986-and-consumer-protection-act-2019/> (Last visited on February 13, 2020).

<sup>129</sup> The Consumer Protection Act, 2019, No, 35 of 2019, India, Acts of Parliament.- s. 2(16), has defined "e-commerce" as buying or selling of goods or services including digital products over digital or electronic network.

Consumer Protection Bill No.1 of 2018. The Bill largely focused on the protection of consumer's interest and settling of the disputes in occasion of issues which are connected or incidental.<sup>130</sup>This Bill was expected to address all the issues relating to consumer protection. The decade old Act of 1986 was aimed to be polished where executive committee was to be proposed to efficiently address all the consumer issues thereby aiming at protection of their interest<sup>131</sup>. It further looks at offering more powers to consumers by increasing liability of the e-Commerce firms. As per this Bill the firms were needed to share more information to the users and disclose how they treat their data, and supports transparency. The bill had also focused on the liability of service providers in e-Commerce where firms shall also be held liable in the event of an error. 'Product liability' was also expected to address the unpredictable and unstable consumer commerce. Consumers engaged in online shopping markets like Airbnb, Quikr and flipkarts were also considered to be addressed under the term 'consumer'. Both traditional and e-Commerce consumers who buy or avail goods and service from brick and mortar stores was also addressed by this Bill. Another objective of this Bill was not other than having a Central Consumer Protection Authority to address the consumer's issues and to be time effective and to provide Suo motu powers to dig into infringement of e-users. The new Act of 2019, which is an Act of the Indian Parliament, has fulfilled this objective by including the term 'Central Authority Council' under Section 3 of Chapter II. The Act has also defined the term "members"<sup>132</sup> which was also defined U/S 2 (1) (jj) of the Parent Act.<sup>133</sup>

---

<sup>130</sup> The Consumer Protection Bill, 2018, *available at* <http://www.egazette.nic.in/WriteReadData/2018/181753.pdf> (last visited on April 12, 2019).

<sup>131</sup> The Consumer Protection Bill, 2018: 7 key rules that will help consumers, *available at* <https://www.indiatoday.in/fyi/story/consumer-protection-bill-2018-7-key-rules-that-will-help-consumers-1414882-2018-12-21> (Last visited on April 13, 2019).

<sup>132</sup> Section 2(27), *Supra* Note 122

<sup>133</sup> Consumer Protection Act, 1986

## 2.4. Techno-legal issues in e-Commerce-Definitional Analysis

The techno-legal issues affecting the privacy and data of individual's in e-Commerce are many. Among the many issues, six techno-legal issues has been discussed below under the headings, (i)**Data Mining** (legal issues of privacy, ethical issues, etc.), (ii)**Cookies** (Cookies and Click Stream Data, Cookies and P3P, Cookies and RFID, Tracking activities of consumers by use Web Cookies), (iii)**Logic bomb, computer viruses, hacking and web bug**, (iv)**Issue involved in transfer of data protection: International data flow**, (v)**Security threats** (Issues of telephone tapping, CCTV: the issue of monitoring, Issues of confidentiality, Exception to breach of confidentiality, Ingredients of confidential information, Obligations of confidentiality: Expressed and Implied, Remedies under common law for breach of confidentiality and (vi)**Issues of Social Networking** ( Facebook, WhatsApp, e-media, press and e-mail).

To understand the above stated six techno-legal issues which are mostly related with data, it is important to understand the terms like data, data bases, sensitive personal data, traffic data, etc. These terms are defined U/S 43 A<sup>134</sup>, 72 A<sup>135</sup> of the Information Technology (Amended) Act, 2008.<sup>136</sup>

---

<sup>134</sup> Section 43 A .- Compensation for failure to protect data. - Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation, not exceeding five crore rupees, to the person so affected. Explanation.- For the purposes of this section,-

(i) "body corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities

(ii) "reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit;

<sup>135</sup> Section 72 A.- Punishment for disclosure of information in breach of lawful contract. - Save as otherwise provided in this Act or any other law for the time being in force, any person including an

The process involving extraction of data from a data base and then converting it into valuable information is known as Data Mining. The developments in different forms of software and hardware systems have enhanced the capacities of the storage devices. The Government, scientific institutions and corporate houses are storing huge volumes of data on a large-scale storage data. The need for protection of such storage devices against corruption, hacking, manipulation, misuse of data becomes a challenging task and the extraction of the data in the event of such incident becomes highly important. The protection of such extracted data against any trespass, theft, misuse or manipulation is a laborious task.<sup>137</sup> In the present-day scenario data mining is also influenced by the law of privacy and social ethics.<sup>138</sup>

There are terms which are necessary to understand the techno-legal issues of privacy and data protection in e-Commerce. Such important terms includes data, data base, sensitive personal data, traffic data, data theft, identity theft, click stream data, data controller, phishing, spam, cloud computing, Blog, whistle-blower, Encryption, adware & spyware and Browsing.

2.4.i. Data: Like the cyber convention, I.T. Act, 2008 has also made an attempt to provide a simple definition of the term “data”<sup>139</sup> as a set of “Knowledge”,

---

intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person shall be punished with imprisonment for a term which may extend to threeyears, or with a fine which may extend to five lakh rupees, or with both.

<sup>136</sup>Niharika Vij, *Law & Technology* 32 (Foreword by Dr. Lalit Bhasin) (Universal Law Publishing, Co. Pvt. Ltd) (2005).

<sup>137</sup> EN Murthy and GRK Murthy Eds. “Data Mining: Legal Implications” (Vol. VIII No. 2) (p.5)(May 2009) (Published on behalf of the ICAI University press, # 52, Nagarjuna Hills, Panjagutta Hyderabad 5000082, Andhra Pradesh) (Printed at M/S. ICIT Software Center Pvt. Ltd., # 1, Andhra Pradesh)

<sup>138</sup>*Id.*

<sup>139</sup> Section 2(1)(o)

“information”<sup>140</sup> and, “facts”. Other important Sections included in this Act are Section 2(1) (t)<sup>141</sup>. The year 2009 can be said to be a progressive year as amendment in the form of Section 43 A<sup>142</sup> was brought up by the I.T. (Amendment) Act, 2009 which was much needed for the protection of privacy in matters of personal data. And gaining statutory recognition and making the intruder liable in the form of Compensation for failure to protect data was another hit step.<sup>143</sup>

2.4.ii. Data Bases: Traditionally Data Bases is regarded to be a one of literally work, including computer programs, tables and compilations, including computer databases. However, recognition of databases in matters of protection of copyrights needs recognition and a separate treatment under the I.T Act.<sup>144</sup>

2.4.iii. Sensitive Personal Data: It is one of the important issues that need to be addressed. This type of data belongs to individual who owns sensitive information about their personal life<sup>145</sup> or information which is per say personal information.<sup>146</sup>

2.4.iv. Traffic Data: Section 69 B<sup>147</sup> of the Information Technology Act, 2008, in its explanation part have put in plain words about what does the term “traffic data” mean.

---

<sup>140</sup> Section 2(1)(v)

<sup>141</sup> “electronic record”

<sup>142</sup> “Compensation for Failure to protect data”

<sup>143</sup> Aparna Viswanatha, *Cyber Law, Indian & International Perspectives*, 31 (Published by LexisNexis Butterworths Wadhwa Nagpur).

<sup>144</sup> T. Ramappa, *Legal Issues in Electronic Commerce* 179 (Published by Rajiv Beri for Macmillan India Ltd.) (2003).

<sup>145</sup> Sensitive information is that information which includes financial (e.g., Account details), sexual (e.g., desire, orientation), medical (e.g., Mental and physical status) and biometric information’s of an individual, *available at*<https://finova.in/privacy-policy.php> (Last visited on February 7, 2020).

<sup>146</sup>The Information Technology Act, 2000 (Act 21 of 2000), s. 43A defines the term “personal information”.

<sup>147</sup> Section 69 B.- Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security.-

(1) The Central Government may, to enhance Cyber Security and for identification, analysis and prevention of any intrusion or spread of computer contaminant in the country, by

This kind of data is given high preferences under this Act as such they are attached to an individual and are of high value. The Convention on Cyber Crime<sup>148</sup> states ‘Traffic Data’ to be a data which is stored in computer, which mostly travels through computer system and contains information<sup>149</sup> Communication resulting in generation of data/computer data is termed as Traffic Data. Such generation of data is facilitated by network or a computer program, system, which is produced by program, system, or network including packet header<sup>150</sup>, pen register<sup>151</sup> and trap and trace data.<sup>152</sup>

2.4.v. Click-stream data: Click stream data: Information collecting agent store about cookies which sends request to their server are click stream data. Huge amount of click stream data is collected using cookies which identifies individual

---

notification in the official Gazette, authorize any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource. (2) The Intermediary or any person in-charge of the Computer resource shall when called upon by the agency which has been authorized under sub-section (1), provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating, transmitting, receiving or storing such traffic data or information. (3) The procedure and safeguards for monitoring and collecting traffic data or information, shall be such as may be prescribed. (4) Any intermediary who intentionally or knowingly contravenes the provisions of sub-section (2) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine. Explanation.- For the purposes of this section.-

(i) "Computer Contaminant" shall have the meaning assigned to it in section 43 (ii) "traffic data" means any data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted and includes communications origin, destination, route, time, date, size, duration or type of underlying service or any other information.

<sup>148</sup> The threat of cyber crime has paved the need for having laws to address the lacunas. Many countries have organized Convention on Cyber Crime and one of such came into existence at Budapest on 23<sup>rd</sup> November 2001. An initiative of the Council of Europe comprising of its member States as well as by other Countries is commendable. 1<sup>st</sup> of July 2004 is remarkable as this Convention came into force on this day. About fifty-three Countries had signed the Convention with twenty-three ratifications on 14<sup>th</sup> of June 2008, available at <https://www.coe.int/en/web/cybercrime/the-budapest-convention> (Last visited on July 23, 2018).

<sup>149</sup>Vivek Sood *Cyber Crimes, Electronic Commerce & Investigation Legal Issues* 243 (Foreword by MR. Goolam E. Vahanvati & 1<sup>st</sup> edition Foreword by Mr. Justice Ajit Prakash Shah) (Published by Ajay Kumar Garg, Nabhi Publication) (2010).

<sup>150</sup> A portion of Internet Protocol is known as packet header that contains address of the data required in reaching the final destination, available at [http://www.info.org/packet\\_header.html](http://www.info.org/packet_header.html) (Last visited on February 7, 2020).

<sup>151</sup> It is a device which functions electronically to record numbers from telephone line, available at [https://en.wikipedia.org/wiki/Pen\\_register](https://en.wikipedia.org/wiki/Pen_register) (Last visited on July 23, 2018).

<sup>152</sup> The IT Law Wiki, available at [http://itlaw.wikia.com/wiki/Traffic\\_data](http://itlaw.wikia.com/wiki/Traffic_data) (Last visited on July, 2018).

computers.<sup>153</sup>The State has a concomitant obligation to define as well as protect data and privacy.<sup>154</sup> Protection of Data will not only protect the privacy but will also help in safeguarding the autonomy of individuals. The landmark judgements in the face of *MP Sharma*<sup>155</sup> and *Kharak Singh*<sup>156</sup> failed to bring into purview the definition of privacy and did not give a place in the pigeon hole of Fundamental rights enshrined in the Constitution of India. Today, 'right to privacy' has gained momentum and is a bench of constitutional happiness. Right to privacy is now part of the Fundamental right by the effort brought in the landmark case of *Puttaswamy*. The judgment emphasizes on the need of having a data protection law and highlights the principle of consent and informational privacy in the era of big brother trend.

2.4.vi. Data theft<sup>157</sup>: It simply refers to unauthorized copying or removal of confidential information from a business or enterprises. Section 43(b) read with Section 66 of the Information Technology (Amended) Act, 2008 deals with offences like "Data Theft".<sup>158</sup>Today people are incurring financial loss with mere prevalence of

---

<sup>153</sup> Click stream data is also known as click path. It is a hyperlink on the website where visitors engage themselves on a featured site. While visiting such site users are also directed to other third party websites which pops on the right hand side of the search engine. Data of the users are captured by such search engines for future purposes and as such privacy of the users are threatened in online world. Consumer's provide their personal information like phone numbers and e-mail addresses while shopping online which are under the constant threat of being misused by third parties for commercial gains. The danger of losing one's privacy is even at greater risk in this technologically driven world, available at [https://en.wikipedia.org/wiki/Click\\_path](https://en.wikipedia.org/wiki/Click_path) (Last visited on July 23, 2018).

<sup>154</sup>Dr. R. Venkata Rao & Dr. T.V. Subba Rao (eds.) *52 A Public Discourse on Privacy-An Analysis of Justice K.S. Puttaswamy v Union of India* (Foreword by Hon'ble Justice Prof. Dr. S. Rajendra Babu) .

<sup>155</sup>*MP Sharma v. Satish Chandra* (1954)

<sup>156</sup>*Kharak Singh v. State of Uttar Pradesh* (1962)

<sup>157</sup>The Information Technology Act, 2000 ( Act 21 of 2000), s. 66B to s. 66F provides punishment for wrongful common activity on the internet. They provide punishment for,

- Dishonestly receiving stolen computer resource or communication device;
- Identity Theft;
- Cheating by personation by using computer resource;
- Violation of privacy;
- Cyber terrorism.

<sup>158</sup>On prove of commission of Data Theft under Information Technology imprisonment is prescribed for those who are found guilty and accused of crimes punishable as per law which is three years that can be extended in some cases and with fine. Such fines may go up to five lakh rupees or both as per copyright Act. Imprisonment is also prescribed in this Act i.e. minimum of six months and maximum



identity theft and the shocking fact is they don't even realize and experience identity theft.<sup>159</sup> Theft (Movable property) has been Anthony Lemar Taylor who had this idea after his 17 years of expertise in petty thefts and first-degree robberies. The identity of Tiger Woods, the greatest golfer was stolen, which was claimed to be a violation of persona by Mr. Wood.

2.4.vii. Identity Theft: In simple terms “is the fraudulent use of another person's identity, mostly for financial gain”<sup>160</sup> and has affected about 7, 00, 000 Americans every year”. America is one of the greatest hubs of Data extraction. To name, Will Smith Basketball Player Steve Smith etc.

2.4.viii. Data controller: When we are talking about data, it is not possible to exclude the terms like ‘data processor or employer of data controller’. This so called data controller is a person who is in charge of processing data on behalf of the owner of data. It is the duty of a data controller to decide the procedure including the purpose and manner which needs to be pursued for the stated task. Even though data controller has access over the data of data owner and they no doubt so process it, it is pertinent to mention here that they do not exercise any control over that data and as such has no responsibility. Calculators, computers are instances of machines that carry out

---

of three years with fine of fifty thousand upto two lakh rupees, *available at* <https://indiankanoon.org/doc/1569253/> (Last visited on July 23, 2018).

<sup>159</sup> Identity theft is a risk to an individual ignited by the online posting of Social Security Number which attracts the thieves. The data brokers causes injury to users on website by insecure handling of their data, *available at* <https://www.investopedia.com/terms/i/identitytheft.asp> (Last visited on July 23, 2018).

<sup>160</sup> Vivek Sood, *Cyber Crimes, Electronic Commerce & Investigation Legal Issues* 136-137.

functions on data and are also referred as data processors. Cloud service providers are now also in the list of data processor.<sup>161</sup>

2.4.ix. Phishing: It refers to deceitful way of getting confidential information.<sup>162</sup> With the advancement in technology many cybercrimes including cyber squatting, cyber bullying, hacking etc. have come into scene causing damages to the economic and personal interest of e-users. One of the most famous of them is ‘Internet Phishing’ which is considered as a criminally wrong course causing the fake websites to prompt the users to disclose their personal information on the con of authenticity or security through an electronic communication with a webpage like that of a legitimate one.<sup>163</sup> Access to personal information has gained momentum after the emergence of social networking sites and in the absence of security indicators, visual deception text, images making underlying text, windows making underlying windows and lack of precautionary guidelines for the users phishers exploit to gather personal information. Phishers obtain sensitive information of customers during online payment services and harms the interest of the net users by causing economic and personal interest.<sup>164</sup> Internet Phishing is a menace which needs a serious attention and monitoring to protect the end users.

2.4.x. Spam: It is uninvited junk in the form of e-mails. They travel through electronic mail boxes with the mensrea of gaining commercial gains.<sup>165</sup> The focus should be not

---

<sup>161</sup> Cloud Service Providers, available at <https://www.techopedia.com/definition/18977/data-processor> (Last visited on 23-07-2018).

<sup>162</sup>Justice Yatindra Singh, *Cyber Laws* 26, (4<sup>th</sup> Edn.) (Universal Law Publishing Co. Pvt. Ltd.).

<sup>163</sup> E.N. Murthy *Internet Phishing: Techno-Legal Approach* 5, GRK Murthy & C Sri Krishna (eds.) (Vol. IX), Nos. 1& 2) *ICFAI J.L. Of Cyber Law* (February and May 2010) (IUP Publications) (Printed at M/S ICIT Software Centre Pvt. Ltd.,).

<sup>164</sup>*Supra* Note at 160.

<sup>165</sup> Sumeet Kumar Singh, “Spamming: Is It Infringement of Privacy” (January- March) (p. 29) (2011 *Cri LJ 1*) [All India Reporter (Pvt. Ltd)].

on the content of the spam but rather on the regulators of spam. Unlike UK<sup>166</sup> till date India do not have Any Criminal codes to regulate such phishing. The I.T Act has no role to play in matters of curbing the menace of Spam though cyber stalking covers spamming, it fails to provide the redressal to the problem. The aggrieved can only go for Section 503, 507 & 508 of the Indian Penal Code. Internet communities are of the view that ‘self -regulation’ is the only way out to address this issue and legal regulation alone will fall short.

2.4.xi. Cloud Computing: According to Wikipedia ‘Cloud Computing’ is a paradigm of Information Technology that offers global access to information.<sup>167</sup>

2.4.xii. Blog: As per Wikipedia ‘blog’ is an online stage facilitated by World Wide Web to discuss and share the views in an informal way and post it from wherever and whenever as the blogger thinks fit.<sup>168</sup> This word was originally termed as ‘Web Log’. Such services are facilitated by no other than the Blog Service Provider who additionally provides the content and make the advertisement. A blogger can share his views, his/her personal experience and knowledge, news on any topic on a website (some topic may be restricted). This technology has replaced the traditional style of writing view/thoughts on one’s diary to the online platform where everyone can have access to any one’s personal view, knowledge and experience. There are varieties of captions given to this term ‘blog’, some of them are tumbler, word press, blogger etc. Here it is to be understood that blogger and blogging are two different things but

---

<sup>166</sup> The UK is having an Act known as UK Fraud Act, 2006 which is explicitly designed to Combat Phishing.

<sup>167</sup>Cloud Computing, *available at* <https://en.wikipedia.org/w/index.php?search=Cloud+computing&title=Special:Search&profile=default&fulltext=1&searchToken=eoukeasc24tm3wyt2xjp9xr9z> (Last visited on July 23, 2018).

<sup>168</sup> Blog, *available at* <https://en.wikipedia.org/wiki/Blog> (Last visited on July 23, 2018).

which are correlated. The former relates to writing of contents for the blog while the latter includes writing of views, expression on any topic. <sup>169</sup>

2.4.xiii. Whistle-blowers: They are persons who reveal or disclose information on the topic and issues like will full misuse of corruption or any sort of information which is often tagged as illegal revelation. Some sections of people termed these sorts of revelations as unethical and bad.<sup>170</sup> There are instances where such Whistle-blowers have been attacked in public and in private, with some witnessing death. To stop this danger the need is felt for keeping their identity safe and behind the curtains. To protect the lives and identity of whistle-blowers, journalists and activists, sites like Wiki leak attains and publish information of sensitive nature.<sup>171</sup>

2.4.xiv. Encryption: According to Wikipedia ‘Encryption’ provides securities against unauthorised access. It encodes information in such a way that only authorized person will have the access. <sup>172</sup>

2.4.xv. Adware and Spyware: The term Adware and Spyware are often used together<sup>173</sup> and there is only a thin line of difference between the two. Adware usually comes with an uninstaller and can be easily removed from a system.<sup>174</sup> The act of collecting information about individuals and even entity without the consent and knowledge is termed as Spyware, facilitated by software. Such software often controls

---

<sup>169</sup>Vivek Sood, *Cyber Crimes, Electronic Commerce & Investigation Legal Issues*.

<sup>170</sup>Whistle Blowers, available at <https://en.wikipedia.org/wiki/Whistleblower> (last visited on 23, 2018).

<sup>171</sup> Wiki Leak, available at <http://www.dictionary.com/e/wikileaks-wikipedia/> (Last visited on 23, 2018).

<sup>172</sup>Encryption, available at <https://en.wikipedia.org/wiki/Encryption> (Last visited on 23, 2018) (at 16:19 PM).

<sup>173</sup> The I.T. Act does not properly address these activities and it is doubtful whether a violator can be punished under s. 43 (c) of the Act or not. And hence this is the grey areas in the Act, which needs to be addressed.

<sup>174</sup>Justice Yatindra Singh, *Cyber Laws*, 23 (4<sup>th</sup> Edn.) (Universal Law Publishing Co. Pvt. Ltd.).

the information of e-consumers and transfers it to third party without obtaining the consent of the data holder. Cookies are the most common example.<sup>175</sup>

2.4.xvi. Browsing: With the help of internet and World Wide Web we can browse from anywhere about anything at just a click of a mouse and interact with anyone around the globe scattered over different jurisdiction. The term browse usually means to look for, and this act is termed as browsing.<sup>176</sup> As information flows from one person to another and within the country to other jurisdiction chances of security breach is very high. Such risks are due to unauthorized access. A breach of security often results when an unauthorized party/individual illegally uses private and confidential information.<sup>177</sup>

#### **2.4.1. Techno-legal issues in privacy and data protection in e-Commerce**

The issue of cyber security is global and far reaching and this issue does not only attract legal hurdle but also do include technical and institutional challenges<sup>178</sup> which needs a comprehensive approach and coherent strategy. The role of different stakeholders and existing initiatives, within a framework of international cooperation is to be considered for protecting critical information infrastructure which is considered to be an integral part of National security.

---

<sup>175</sup> Spyware, available at <https://en.wikipedia.org/wiki/Spyware> (Last visited on July 23, 2018).

<sup>176</sup> Browser, available at <https://searchwindevelopment.techtarget.com/definition/browser> (Last visited on July 23, 2018).

<sup>177</sup> Confidential Information, available at <https://www.techopedia.com/definition/29060/security-breach> (Last visited on July 23, 2018).

<sup>178</sup> Prashant Mali *Cyber Law & Cyber Crimes* 2, Information Technology Act, 2000 With New IT Rules, 2011

As stated in the introductory Supra at page 52, techno-legal issues in privacy and data protection in e-Commerce includes six techno-legal issues, supra they are discussed as follows:-

#### 2.4.1. i. Data Mining

Contemporary era decorated with internet has facilitated the flow of data not only from the government but private organisations too. Huge information in the form of data ranging from sensitive to personal are collected for illegal purposes without the knowledge of data holder. Such illegal act of data extraction has attracted the serious need for security. Crimes facilitated on online platform have been a major concern over the years all over the country which needed a law to address the same was felt by India too. As a result the Information Technology (Amended) Act, 2008, with section 43-A is seen as a guiding torch for protecting privacy of individual's information which is held by private intermediaries. Further it tries to prevent unauthorised disclosure of "sensitive personal data or information."<sup>179</sup>

Apart from the issue of Privacy, issue of security have been an inseparable one in e-Commerce and include struggled access by the unauthorized other of the data belonging to another and is one of the critical problems for e-Commerce users.<sup>180</sup>The techno-legal issues of data mining also include issues of privacy and ethical issues.

In today's world Data and Information have become a central part of everyday life. Personal sensitive information like addresses, financial details, and health records among others are often targeted for illegal gains. Privacy and data protection regime are desired to secure privacy and information of consumers across the Country and

---

<sup>179</sup> Rishika Taneja and Sidhant Kumar, *Privacy Law* 257.

<sup>180</sup>Mehrdad Ghayoumi, "Review of Security and Privacy Issues in e-Commerce", *available at* <http://worldcomp.proceedings.com/proc/p2016/EEE6029.pdf> (Last visited on June 8, 2017).

even at international borders where information is travelled without knowledge of the consumers. In the event of obtained consent issue arise where the collected information are used for other than the consented purposes. A law is the only secure way to protect the vulnerable rights of the citizens.<sup>181</sup>

Social and organizational issues also holds a place while talking about security issues it covers “security policies, separation of duties, security assurance and access control. Other concern is that of the weak link in security and is often associated with employees or users, rather than the technology and lastly is the software engineering management or managing how security technology is deployed”.<sup>182</sup> Security is regarded by researchers as the core issue that hinders e-Commerce growth.<sup>183</sup> Due to security concern and issue of data theft consumers are hesitant to indulge themselves on an online activity which in return affects the e-Commerce. Apart from educating the consumers on issue of security an effective law is also needed to gain their confidence. Denial of service<sup>184</sup>, –unauthorized access<sup>185</sup>, and theft<sup>186</sup> and fraud are the most common security threats.<sup>187</sup>

---

<sup>181</sup> Rishika Taneja and Sidhant Kumar, *Privacy Law*.

<sup>182</sup> Ms. Palak Gupta and Dr. Akshat Dubey, *E-Commerce- Study of Privacy, Trust and Security from Consumer's Perspective* 224-232 (Vol.5 Issue 6, June) (2016), available at <http://www.ijscmc.com/docs/papers/June2016/V5I6201647.pdf>, (Last visited on June 18, 2017).

<sup>183</sup> Kuldeep Kaur et al, “*E-Commerce Privacy and Security System*”, (Vol.5, Issue 5, Part-6) May (p. 63-73), (2015) [http://www.ijera.com/papers/Vol5\\_issue5/Part%20-%206/J505066373.pdf](http://www.ijera.com/papers/Vol5_issue5/Part%20-%206/J505066373.pdf) (Visited on June 20, 2017).

<sup>184</sup> D.O.S. attack means preventing the legitimate users of a service from availing it. And such an Act is covered under s. 66 of the I.T. (Amended) Act, 2008. Such an activity does not cost information security but do cost time and money.

<sup>185</sup> When some person other than the authorised individual makes an unauthorised access it is then described as unlawful access which lacks consent of the rightful owner, available at <https://www.computerhope.com/jargon/u/unauacce.htm> (Last visited on January 15, 2019).

<sup>186</sup> According to Wikipedia, theft is the taking of another person's property or services without that person's permission or consent with the intent to deprive the rightful owner of it, *Mens Rea* in offences against Property, available at [https://shodhganga.inflibnet.ac.in/bitstream/10603/132472/10/10\\_chapter%205.pdf](https://shodhganga.inflibnet.ac.in/bitstream/10603/132472/10/10_chapter%205.pdf) (Last visited on January 15, 2019).

<sup>187</sup> According to Wikipedia, fraud is an act which is intentionally committed by a person to secure gains unlawfully, available at <https://en.wikipedia.org/wiki/Fraud> (Last visited on December 18, 2017).

As in coal mining labour extracts coal from the mines, data are extracted from the computer with the help of technology; such an act is termed as Data mining. Such data are usually in raw form. In this act of extraction privacy and sensitive information of individual are often compromised. <sup>188</sup> Data mining has paved way for social issues in addition to technological one. It is social as it involves privacy of individual. Data quality, data mining, interoperability, privacy laws and regulations are the issues in Data Mining and also include <sup>189</sup> prediction, regression, classification, link analysis, clustering, Exploratory Data Analysis (EDA), model visualization, Summarization, and dependency modeling among other challenges.<sup>190</sup>

Talking about India a large number of telemarketing<sup>191</sup> is unsolicited. The menaces of unsolicited calls were brought up in the case of *Harsh Pathak v. Union of India* and others<sup>192</sup>. In this matter, the Reserve Bank of India, vide Notification No *RBI/2013-14/136 DBOD.No.FSD.BC.30/24.01.001/2013-14 dt.July 15, 2013*,<sup>193</sup> released a

---

<sup>188</sup> Anmol Kumar, Amit Kumar Tyagi, *et.al.*, (Volume 4, Special Issue 1, February 2014), available at [http://www.ijetae.com/files/ICADET14/IJETAE\\_ICADET\\_14\\_01.pdf](http://www.ijetae.com/files/ICADET14/IJETAE_ICADET_14_01.pdf) (Last visited on June 27, 2017).

<sup>189</sup> Dileep Kumar Singh & Vishnu Swaroop, "Data Security and Privacy in Data Mining: Research Issues & Preparation" (volume 4, Issue2- 2013), available at <http://ijctjournal.org/Volume4/issue-2/IJCTT-V4I2P129.pdf> (Last visited on June 27, 2017).

<sup>190</sup> Srivathsa Gottipati, "Exploratory Data Analysis (EDA)", available at <https://medium.com/@srivathsa/srivathsa-gottipati/exploratory-data-analysis-eda-4b81d84ef5cf> (Last visited on December 16, 2019)

<sup>191</sup> In Telemarketing customers are directly in contact with the seller, it is a direct form of marketing. Customers either buy products online or call the seller for the delivery of the product. Some telemarketing also involves recorded sale programme through automatic dialing. This form of marketing is facilitated by internet as well as telephone/Mail., available at <https://en.wikipedia.org/wiki/Telemarketing> ((Last visited on December 16, 2019).

<sup>192</sup> In this Case, the Hon'ble Supreme Court directed telemarketer's to register themselves with Department of Telecommunication (DoT) and those who fails was not be permitted to operate in the telemarketing services. Non-adherence with the above criteria was regarded as the violation of Hon'ble Supreme Court's above direction, available at <https://economictimes.indiatimes.com/telemarketing-and-unsolicited-calls/articleshow/1670382.cms?from=mdr> (Last visited on December 16, 2019).

<sup>193</sup> Unsolicited Commercial Communications -National Customer Preference Register (NCPR) (Updated on July 20, 2013), available at <https://simplybanking.wordpress.com/2013/07/20/unsolicited-commercial-communications-national-customer-preference-register-ncpr/> (Last visited on December 16, 2019).



mandatory norms to all the banks to get itself with only the registered telemarketers. Those banks were also to follow the TRAI guidelines time and when needed.

#### 2.4.1.ii. The issue of Cookies

A cookie is a tiny readable machine text file on computer. Cookie contains some identifier (ID Number, name) along with other information which allows the extractor both to personalize treatment of the user and to collect information about that user's behavior on the site. Cookies not only confer benefits to the users but also the collecting agent. Cookies help the extractor to personalize user experience and to collect certain data about user behavior. First party usually places a cookie on a user's computer. Third parties like advertisers may also do that. Another thing is such information may or may not be collected anonymously. Third party cookies<sup>194</sup> associate the information with unique but anonymous, identifier and do not contain personally identifiable information.<sup>195</sup> 'A cookie is just an identification number like a bar code that a collecting agent writes to a user's computer'.<sup>196</sup>

#### 2.4.1.iii. The issues of tracking activities of consumers by use of web cookies

The moment individuals share their information on internet, it is no more private,<sup>197</sup> as this information are just one click away from others and is easily available through search engines to other users as well as to internet service providers and service

---

<sup>194</sup> Cookies are actually a device to help the Web providers and the users. All agents in a website have their own cookie. Cookies help anyone from anywhere to track the user's activities. Some websites asks for user's consent, some don't. Information's viewed by individuals are stored by these cookies and are used in future for delivering the required page. Talat Fatima, *Cyber Crimes* 210 (EBC Publishing Pvt. Ltd.) (2016).

<sup>195</sup> Lee Kovarsky, "Tolls on the Information Superhighway: Entitlement Defaults for Click stream Data" (RYAN STORES et al editor) (VIRGINIA LAW REVIEW) (Vol. 89:1037) (No. 5) (4-6) (1046-1047) (2003).

<sup>196</sup> *Supra* Note at 188.

<sup>197</sup> Karnika Seth, *Computers, Internet and New Technology Laws* 281, A Comprehensive work with a special focus on developments in India, (1<sup>st</sup> Edn.).

providers who owns various websites<sup>198</sup>. The advent of technology has led to an unprecedented emphasis on data and information<sup>199</sup> and Web sites dealing with e-business have become technologically smarter consequently facilitating the tracking of the activities of a consumers using a Web page supported by a stunning feat called “cookies”<sup>200</sup> and therefore records the user’s Web site, e-mail address, buying behavior and all other data including customizable information.<sup>201</sup> “Cookies” are portrayed as a small file of letters and numbers that acts as an identifier which are often used in counting the number of hits on websites and it also plays as a key part of the way most on-line shopping baskets work containing details of the website server which had planted the cookie, along with date and time as well as life time of a cookie with additional information’s.<sup>202</sup> As human interactions increasingly go online, privacy protection is a primary concern. The amount of data we generate online and its vulnerability to misuse creates a new challenge for legal and regulatory framework.<sup>203</sup> The use of cookies, which are installed on hard drive of a user is popular in behavioral advertising<sup>204</sup> and though cookies can be detected and can be removed from a system with the help of web browser and software products, still some data of sensitive nature are being reported to have been passed by cookies which have then been used by various Advertising Agencies without prior permission from

---

<sup>198</sup> *Id.*

<sup>199</sup> Rishika Taneja and Sidhant Kumar, *Privacy Law* 231.

<sup>200</sup> Raman Mittal and Neelotpal Deka, *Cyber Privacy, Legal Dimensions of Cyberspace* 214 (S.K. Verma & Raman Mittal (eds.), (Published by Prof. (MS) S.K. Verma for Indian Law Institute).

<sup>201</sup> *Id.*

<sup>202</sup> Richard Morgan & Ruth Boardman, *Data Protection Strategy, Implementing Data Protection Compliance* 90(Published by, Sweet & Maxwell, 2003, London NW3 3PF) (2003).

<sup>203</sup> Rishika Taneja and Sidhant Kumar, *Privacy Law* (231).

<sup>204</sup> When a user visits a web page that it has already visited before, the cookie data will point out the same. The web site once revisited will capture the cookie data and advertise its products or services which will be of interest to a user. This concept is known as behavioural advertising, *available at* <https://neilpatel.com/blog/behavioral-advertising/> (Last visited on March 23, 2019).

the concerned members from social networking sites like Facebook<sup>205</sup>, thereby taking a place of serious concern for International Organisations which deals with privacy laws and for this reason it has been criticized for selling personal data for unrelated commercial gains without any permission.<sup>206</sup> In general, a cookie usually aids the Web sites to serve users better and in no way their existence is concealed from them as the user can easily disallow access to cookie information<sup>207</sup>, the problem arises when the Web sites stores the information one is unaware of and it is where a cookie becomes a threat and is considered to be a spyware.<sup>208</sup> Consent of the users while tracking activities with cookies is another issue in e-Commerce.<sup>209</sup> Misuse of cookies regards to its flexibility<sup>210</sup> and it also lacks security. The term 'cookie' is referred to information which a Website place on e-users hard disk with a motive to retain information about that user for future use. To be more specific, a cookie records one's personal preferences over the websites thereby using the Web's Hypertext Transfer Protocol (HTTP) and each request made on the web page is independent of all other requests and hence record of visited pages and anything related to the search cannot be traced.<sup>211</sup> To sum up a cookie acts like a device and facilitates a server to store information of a user on user's own computer and in that way the user can view the cookies that have been so stored.<sup>212</sup> A Cookie is a small file placed by a Web page on a computer visiting that page. Cookies generally contain information about the visited

---

<sup>205</sup> Karnika Seth, *Computers, Internet and New Technology Laws*, 281 A Comprehensive work with a special focus on developments in India, (1<sup>st</sup> Edn.), LexisNexis.

<sup>206</sup>*Id.*

<sup>207</sup>Raman Mittal and Neelotpal Deka, *Cyber Privacy, Legal Dimensions of Cyberspace* 215 (S.K. Verma & Raman Mittal (eds.), (Published by Prof. (MS) S.K. Verma for Indian Law Institute).

<sup>208</sup>*Id.*

<sup>209</sup> Paul A. Watters, *Taming the Cookie Monster* (2012), available at <http://www.canberra.edu.au/cis/storage/Taming%20the%20cookie%20monster-%20FINAL.pdf> (Last visited on June 22, 2017).

<sup>210</sup> Emil Sit & Kevin Fu, "Web Cookies: Not Just a Privacy Risk", (September 2001/Vol. 44, No. 9), available at <https://courses.cs.washington.edu/courses/cse484/14au/reading/cookies-risk.pdf>, (Last visited on July 4, 2017).

<sup>211</sup> Raman Mittal & Neelotpal Deka, *Cyber Privacy" Legal Dimensions of Cyberspace* 214 S.K. Verma & Raman Mittal (eds.), (Published by Prof. (MS) S.K. Verma for Indian Law Institute).

<sup>212</sup>*Id.*

computer. They can store information such as passwords and preferences or pages previously viewed. Cookies collect information about web browsing by individual users and because they remain on a computer for long after a page is visited, they can raise security and privacy concerns. Cookies can be used in conjunction with adware and spyware to track a user's online and offline computer use, it can also track Web pages viewed and documents opened, and the adware or spyware can then transmit that information to some third party.<sup>213</sup>

Cookies even track<sup>214</sup> people and get information as users leave a footprint of personal choices and preferences leaving a profound impact on privacy of Web site visitors.<sup>215</sup> A cookie no doubt is beneficial to both the users and Web providers, but on the other side it is also accompanied with vulnerability of being misused as many users don't know beyond its existence.<sup>216</sup> The I.T. Act does not deal with issues of cookies directly<sup>217</sup> but has made an attempt to cover it under the purview of section 43(A).<sup>218</sup> Whereas, there are directives in European Parliament on Electronic Communications<sup>219</sup> on implementation of the Privacy and Electronic Communications Regulations<sup>220</sup>, which contains specific rules on the use of cookies

---

<sup>213</sup> Ian J. Lloyd, *Information Technology Law* 53 (7<sup>th</sup> Edition) (Published by, Oxford University Press 198 Madison Avenue, New York, United States of America) (2014).

<sup>214</sup>Raman Mittal and Neelotpal Deka, *Cyber Privacy Legal Dimensions of Cyberspace* 215 (S.K. Verma & Raman Mittal (eds.), (Published by Prof. (MS) S.K. Verma for Indian Law Institute).

<sup>215</sup>*Id.*

<sup>216</sup>*Supra* Note at 213.

<sup>217</sup>*Id.*

<sup>218</sup> The Information Technology Act, 2000 (Act 21 of 2000), s. 43 A, Compensation for Failure to Protect Data. - Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected. \*[Inserted by The Information Technology (Amendment) Act, 2008 (10 of 2009) (w.e.f. 27-10-2009)].

<sup>219</sup> Directive 2002/58/EC of the European Parliament under the Council of July 12, 2002, published in the official journal on 31, 2002.

<sup>220</sup> Regulations 61(1) and (2) of the E.U. Directives provides that- (1) Subject to paragraph (4), a person shall not use an electronic communications network [i.e. the internet] matters relating to information

and similar devices. As per the Electronic Communications (EU Directive) Regulations 2003 (made on September 18, 2003) an Organisations using ‘cookies’ call for inclusion of additional information in their fair obtaining notices to get compilation with the said EU Directives.<sup>221</sup> Apart from these guidelines, attention is given on the ‘tracking of the activities’ by the tracking technology such as ‘cookies’ in considering the online privacy by the Guidance given by the Article 29 Data Protection Working Party<sup>222</sup>, which emphasize on alerting an individual regarding this information during the time of collection of personal data and further points out the importance of including cookies in a privacy statements.<sup>223</sup>

#### 2.4.1.iv. Cookies and Platform for Privacy Preferences (“P3P”)

The Platform for Privacy preference Project (p3p) is regarded as an old-fashioned protocol which allows websites to uphold their intention in using the information they collect about web browser users. It was developed by World Wide Web Consortium

---

storage and unlawful use of those saved information. Such information relates to a subscriber or user unless the requirements of paragraph (2) are met. -

a. is provided with clear and comprehensive information about the purposes of the storage of, or access to, that information; and b. is given the opportunity to refuse the storage of or access to that information.”

Cookies fall within paragraph 6(1) as they are files of information transmitted via the Internet and stored on an end user’s terminal. Regulation 6(2) requires any organization that uses cookies to have a cookie statement and to provide that users must be able to refuse to accept a cookie. The DTI has deliberately tried not to be prescriptive as to how organisations to reject the obligation. There are some exceptions and limitations to the information and rejection provisions. Firstly, Regulations 6 (3) provides that if an organisation wishes to use cookies whenever an individual visit its site, it provides the information and opportunity to reject a cookie only on the initial visit. Secondly, Regulations 6 (4) provides that there is no need either to provide the information or the opportunity to reject a cookie where use of a cookie or similar technology is “a. For the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network; or b. ....strictly necessary for the provision of an information society service requested by the subscriber or user”. The exception at paragraph (b) would cover cookies that are required for the provision of websites services-for example where a cookie is required in order to run an online shopping basket.

<sup>221</sup> Richard Morgan and Ruth Boardman, *Data Protection Strategy, Implementing Data Protection Compliance* 90-91 (Published by, Sweet & Maxwell, 2003, London NW3 3PF) (2003).

<sup>222</sup> Recommendation 2/2001 on certain minimum requirements for collecting personal data on-line in the European Union May 17, 2001, (6).

<sup>223</sup> Richard Morgan and Ruth Boardman, *Data Protection Strategy, Implementing Data Protection Compliance* 91-91 (2003).

(W3C) and gained recommendation in the year 2002. Microsoft Internet Explorer and Edge were the only major browsers to support P3P as there was hardly any development in the implementation of the same. As a cookie handling protocol P3P is recently used by Internet Explorer 6.0.<sup>224</sup> Six shades of cookie handling settings are available in the Internet Explorer Software 6.0, which exclusively deals with cookie issues. The e-Users/ consumers may choose from the six taxonomies, viz; accept all cookies, low, medium, medium-high, high, and block all cookies. Among them medium is the default setting, which blocks any cookies from servers without compact privacy policies.<sup>225</sup>

#### 2.4.1.v. Cookies and Radio-Frequency Identification (RFID)

Cookies<sup>226</sup> are tracking tag generating a code on the basis of shopping habits and preferences. Companies<sup>227</sup> generates codes and place it in a cookie to track the activities of the people while RFID<sup>228</sup> is a technology that allows objects around us to be sensed and observed by computers and in other sense a radio platform to communicate<sup>229</sup>. It has become pervasive at its nascent stage and linked with Internet

---

<sup>224</sup> Lee Kovarsky, *Tolls on the Information Superhighway: Entitlement Defaults for Click stream Data* (RYAN STORES et al editor) (Virginia Law Review) (Vol. 89) (No. 5) (4-6) (1082) (2003).

<sup>225</sup> Under the P3P cookie-handling functionality deployed by Explorer, when a user first types the URL address into the browser, the browser requests a privacy policy reference file from all collecting agents (domains) serving cookie content into the web page. These agents generally consist of the website and any affiliates or advertisers also serving code into that page. If the site has what is called a “compact privacy policy,” the collecting agent will return the reference file detailing the location of that policy to the browser...If a collecting agent attempts to set a cookie that is either blocked or downgraded by the browser, a little red icon signaling that event appears in the bottom right corner of the screen. If the user wishes to investigate the specifics of the rejection or modification, she can click on that icon for a report.

<sup>226</sup> Dennis Marks “What is the difference between Cookies and Tracking Tags” (March 22, 2018) available at <https://www.quora.com/What-is-the-difference-between-cookies-and-tracking-tags> (Last visited on October, 4, 2018).

<sup>227</sup> There are problems of unwanted ads in the websites which are often browsed by the consumers while engaging themselves in selling companies. The choices and preferences are well known by the websites without our free known given consent.

<sup>228</sup> It provides unique wireless identification for objects identifiable by computers.

<sup>229</sup> MIT (Massachusetts Institute of Technology) Technology Review, available at <https://www.google.co.in/search?q=MIT&oq=MIT&aqs=chrome..69i57j69i61j014.1351j0j7&sourceid=chrome&ie=UTF-8> (Last visited on 04.10.2018).

of Things (IOT) creating a platform. By reason of its capabilities in identification of tracking items, unique identification for item has been comprehensively deployed.<sup>230</sup> Today RFID is tagged as “THE NEXT BIG THING.”<sup>231</sup> It is a technology that helps in the secret study possible. RFID is not new, as its presence can be traced back to World War II, where British army used it to recognize friendly aircraft and is also a technology familiar in the north eastern United States enabling the EZ-Pass<sup>232</sup> toll payment system. RFID is a wireless identification which is often used in Car keys, laptops, passports, students ID, Retail shops (clothes and shoes etc.), Payment system, manufacturing, Inventory management, wireless tracking, Asset tracking. The most common device using RFID is our mobile phones (IMEI)<sup>233</sup>. It sends signals to RFID tags<sup>234</sup> and receives and decodes information from them.

We know that our privacy is under attack <sup>235</sup> “The problem is we don’t know how to fight back” is the line sensed by Simon Garfinkel in his writing titled “*Database Nation*”.<sup>236</sup> The Privacy issues in RFID is that of Real-time tracking of the activities

---

<sup>230</sup>Nimish Vartak, Anand Patwardhan, *et.al*, “Protecting the Privacy of Passive RFID tags”, *available at* <https://pdfs.semanticscholar.org/2b44/c877d53d27ebc4a0f810f562000a28813794.pdf> (Last visited on October 3, 2018).

<sup>231</sup> It also came to be known as the Broken Arrow Affair.

<sup>232</sup>E-ZPass was created in the year 1987 and is used by the U.S., in mostly roads and bridges and is facilitated by electronic system. This system is operated at 17 states and it also facilitates the travelers to use the same transponder on toll roads throughout the network, *available at* [https://en.wikibooks.org/wiki/Transportation\\_Systems\\_Casebook/Tolling/E-ZPass](https://en.wikibooks.org/wiki/Transportation_Systems_Casebook/Tolling/E-ZPass) (Last visited on October 04, 2018).

<sup>233</sup>The International Mobile Equipment Identity, in short IMEI is a number, usually unique, to identify Global System for mobile Communication (GSM), Wideband Code Division Multiple Access (WCDMA), and iDEN (integrated Digital Enhanced Network), mobile phones, as well as some satellite phones. It is usually found printed inside the battery compartment of the phone, Amarnath Mitra, “*RFID in India: Implementation, Issues and Challenges*”, *available at* <https://imanagerpublications.com/index.php/article/2942> (Last visited on August 20, 2018).

<sup>234</sup> RFID tags are further divided into active and passive. The former receives power from RFID reader; Transmission is depended on power from RFID reader, whereas the latter one has their own power supply; can transmit data independently of RFID reader.

<sup>235</sup> Jan Henrik Ziegeldorf, Oscar Garcia Morchon, *et.al*, *Privacy in the Internet of Thing: Threats and Challenges*, *available at* <https://arxiv.org/ftp/arxiv/papers/1505/1505.07683.pdf> (Last visited on October 04, 2018).

<sup>236</sup> Laura Hildner “Defusing the Threat of RFID: Protecting Consumer Privacy, Through Technology-Specific Legislation at the State Level” (Eun Young & Jocelyn Simonson et al Edtrs.) (*Harvard CIVIL*

of the people, coupled with implanting the tags within the bodies without the knowledge of the customers/people, Criminal activities using RFID readers, where they read items on someone's house along with personal information like medical information etc. by implanting tags. There is a fear among people popularly captioned as "Big Brother is watching us". The fear concerning RFID and Privacy is largely unfounded and Information Technology Act should be molded to suit the challenges posed by the RFID to check data leakage.<sup>237</sup>

#### **2.4.2. Issues of Logic Bomb, Computer Viruses, Hacking & Web Bugs.**

Another way of tracking activities or information is by use of a logic bomb. In case of logic bomb there is an intentional attaching of a piece of code into a software system and when specific conditions are met it will automatically set off a malicious function. For example, a programmer may hide a piece of code that starts deleting files (such as a salary database trigger). There are innumerable issues attached with computer system that hampers the information of users. One of such issues is of 'computer viruses. This computer virus modifies and even copy computer programs by way of inserting its own code. It infects the system thus affecting the areas it had targeted.<sup>238</sup>

According to Wikipedia, Unauthorised access<sup>239</sup> to gain access to a computer system by way of improper means is termed as hacking."<sup>240</sup> Douglas Thomas is of the idea that, 'Cyber Crime has, and in many ways, become synonymous with hacker and

---

*RIGHTS, CIVIL LIBERTIES LAW REVIEW Vol. 41, Winter 2006* (1-2 (No. 1)2006) (Publication Centre: Harvard Civil Rights-Civil Liberties Law Review, 1541 Massachusetts Avenue Cambridge, MA 02138 (617) 495-4500).

<sup>237</sup>Jeremy James "Privacy and RFID" (Published in Mar. 25, 2013), *available at* <https://www.youtube.com/watch?v=UMFXce79PD0> (Last visited on October 04, 2018).

<sup>238</sup> Computer Virus, *available at* [https://en.wikipedia.org/wiki/Computer\\_virus](https://en.wikipedia.org/wiki/Computer_virus) (Last visited on July 23, 2018).

<sup>239</sup> Hacking is another term which can be used for unauthorised access.

<sup>240</sup> Lewis Morgan, "Hacking v Unauthorised access-What's the difference?" (26<sup>th</sup> June 2015), *available at* <https://www.itgovernance.co.uk/blog/hacking-vs-unauthorised-access-whats-the-difference/> (Last visited on August 10, 2018).



hacking'. Hackers<sup>241</sup> are regarded to be a dignified and talented offender in a cyber world. In practice Hacking is technical know-how and expertise and are different from cyber criminals. The *actus reus* of hacking coupled with criminal mensrea amounts to cybercrime.<sup>242</sup>

GIFs are recent development or say an example of Web Bugs. It is a tiny graphic, included in a web page or e-mail messages which identify who or how many people are viewing the material. They are usually small with clear images without visible content. They are usually tagged and placed in the image of the underlying HTML code of the page and is also placed in HTML-enabled e-mail messages.<sup>243</sup>

#### **2.4.3. Issues involved in transfer and data protection: International Data flow.**

When our data stays within our Country, there is a control over it, the problem starts once our data leaves the boundary and falls under various jurisdiction. The largest digital payment system of our Country has taken the shape of 'Paytm'. Due to concern for consumer's data, it is praying the Government to keep the customer's data within country's jurisdiction only.<sup>244</sup> An entity such as WhatsApp<sup>245</sup> is blown by the norms of the R.B.I.<sup>246</sup>

---

<sup>241</sup> Hackers are those individuals who without any authority hacks and access the computer containing information stored on it and pose threats to all those who put their information online. Any loopholes in the computer program is a gateway to these hackers to threaten the security of the information's, Suriya Begum, Sujeeth Kumar, *et al.*, *A Comprehensive Study on Ethical Hacking*, available at <http://www.ijesrt.com/issues%20pdf%20file/Archive-2016/August-2016/21.pdf> (Last visited on July 23, 2018).

<sup>242</sup>Sundargopal Ghoshal "A Study of Legal control of Cyber\_Crimes with special reference to the Information Technology Act" (2005), available at [http://shodhganga.inflibnet.ac.in/bitstream/10603/64010/5/05\\_contents.pdf](http://shodhganga.inflibnet.ac.in/bitstream/10603/64010/5/05_contents.pdf) (Last visited on August 13, 2018).

<sup>243</sup>Yee Fen Lim, *cyberspace law* 133 (Publication Oxford University Press) (2008).

<sup>244</sup> Pratik Bhakta "Insists on local storage of data, Paytm tells govt." (July 24, 2018), available at <https://economictimes.indiatimes.com/small-biz/startups/newsbuzz/insist-on-local-storage-of-data-paytm-tells-govt/articleshow/65112783.cms> (Last visited on August 10, 2018).

<sup>245</sup>Pratik Bhakta, "WhatsApp had said it uses the Facebook platform to process United Payments Interface transactions originating out of India", (Last Updated, July 24, 2018), available at

#### 2.4.4. Security Threats

Privacy is about keeping information and data confidential.<sup>247</sup> Denial of Service (Dos) attacks is the most common form of threat to IoT (Internet of Things)<sup>248</sup>. New technologies mean new threats to security with the advance attacking tools which initiates a reason to make ‘security’ the main topic for discussion and protection at large. Section 69<sup>249</sup> and, 69 (4)<sup>250</sup> is regarded as the most significant amendments made in the I.T. Act, 2000. The later Section under sub-section (2) of this Act, makes an intermediary liable if he/she “*intentionally*” acts contradictory to the laid down provisions of this Section. And for investigation of any offences, the I.T. (Amendment) Act, 2008 is regarded as important which concerns itself to the provisions of security.<sup>251</sup>

With the help of internet e-commerce in India is growing remarkably and has invited many legal issues of security. As security plays an important role in promoting e-Commerce, the regulatory frameworks in India are addressing the same. They include I.T. Act, Indian Contract Act and Indian Penal Code. In India online shopping requires compliance with banking and financial norms too. PayPal is one of the

---

<https://economictimes.indiatimes.com/small-biz/startups/newsbuzz/insist-on-local-storage-of-data-payment-tells-govt/articleshow/65112783.cms?from=mdr> (Last visited on August 10, 2018).

<sup>246</sup> For check and balance of transaction R.B.I. in the month of April, 2018 appealed every companies operating in India relating to payment to come up with facilities that would help storage of data. For this task six months time was provided. This initiative aimed at bringing an uninterrupted supervision over the management and transaction of data which would end up in smooth networking system.

<sup>247</sup>Rolf H. Weber and Romana Weber *Internet of Things Legal Perspectives* 43(Published by Springer-Verlag Berlin Heidelberg) (2010).

<sup>248</sup> In Internet of Things, both privacy and security are considered to be of prime importance. Here, fair competition is ensured by maintaining confidentiality of the transactions and involved enterprises. Security measures are also adhered to in the IoT to check attacks, threats to the system, and to ensure safety of the information at national and international level, Rolf H. Weber and Romana Weber, *Internet of Things, Legal Perspective* (Published by Springer-Verlag Berlin Heidelberg) (2010).

<sup>249</sup> “Powers to issue directions for interception or monitoring or decryption of any information through computer resource”

<sup>250</sup> The Information Technology (Amended) Act, 2008

<sup>251</sup>Vivek Sood *Cyber Crimes, Electronic Commerce & Investigation Legal Issues* 184 (Foreword by MR. Goolam E. Vahanvati & 1<sup>st</sup> edition Foreword by Mr. Justice Ajit Prakash Shah) (Published by Ajay Kumar Garg, Nabhi Publication) (1<sup>st</sup> Edn.) (2010).

examples of online payment system in India that has to allow payment receipt and disbursements for its existing or proposed e-Commerce business and have to take license from Reserve Bank of India (R.B.I.).<sup>252</sup> The recent advancement in the past decade in the area of cyber is that of Online Social Networks (OSNs)<sup>253</sup> and popular players are face book, Twitter, LinkedIn, Pinterst, MySpace etc<sup>254</sup>.

#### 2.4.4.i. Issues of Telephone Tapping

People have always admired and respected their privacy. Privacy is not a new concept but has gained prominence in today's world due to the immense advancement in the internet playground. The term privacy differs from person to person and is not limited to a defined geographical area. Each Country has their own weapon to deal with the menace of privacy intrusion and data protection. Some scholar narrated privacy as “a wish to remain unnoticed in the public realm”<sup>255</sup>. In a Society human beings are inevitable and so is the conflict. In the era of technology where everything is available

---

<sup>252</sup> K. Susheel Barath & Dr. V. Mahalakshmi, “Legal Issues in e-commerce transactions –An Indian Perspective”, 185, (Volume 4, Issue 11,) (International Journal on Recent and Innovation Trends in Computing and Communication), *available at* <https://ijritcc.org/index.php/ijritcc> (Last visited on December 13, 2020).

<sup>253</sup> In comparison to the real world where information is ephemeral, the information on the web remains for an infinite time thereby posing a great risk on the privacy of online users. Most of the time users are unaware of the potential risks involved when they are sharing sensitive information online. Whenever and wherever the Personal Identifiable Information (PII) is shared and stored, privacy concerns are bound to arise. Hence, it is difficult to preserve privacy in a domain like OSN which is inherently designed for sharing. Leak in sensitive data could result in lawsuits, loss of customers' confidence, brand damage, erosion of privacy, bad press, loss of revenue etc. Photos and videos from the profiles could be morphed and used for threatening, blackmailing and defaming individuals. Likes and interests reveal a lot about a person and can lead to the formation of controversial opinions. Using address, the schedule of a person could be known which can result into a criminal attack or burglary. Social Security Number (SSN) of individuals could be determined using a combination of address, date of birth and gender resulting in ID theft or impersonalization. E-mails and phone numbers could be misused for targeted advertising leading to unnecessary interruptions and spam. Study of privacy if viewed from the prism of privacy enhancing algorithms has a lot of missing links and is a topic of high relevance. Hence, it is a great challenge to protect the confidential and sensitive data from unauthorized users and ensure that the actual data is available to the legitimate users as well, Agrima Srivastava, *Enhancing Privacy in Online Social Networks using Data Analysis* (2015) (Unpublished Ph.D. thesis, Birla Institute of Technology, Pilani)

<sup>254</sup> Agrima Srivastava “Enhancing Privacy in Online Social Networks using Data Analysis” (2015), *available at* <http://shodhganga.inflibnet.ac.in/bitstream/10603/125427/1/synopsis.pdf> (Last visited on September 4, 2018).

<sup>255</sup> Parveen & Rehana “Protection of Privacy in India: Law and juridical Concerns” (2010), *available at* <http://shodhganga.inflibnet.ac.in/handle/10603/52364> (Last visited on October, 03, 2018).

at the click of a button, Individuals privacy and data are at threat and is in conflict with the easy accessibility of information anywhere and from everywhere without the consent of the legal owner. Human beings are social animals and live in a society, but this social animal also needs privacy which at any cost needs to be protected and respected at the same time. They are issues which have crippled the privacy at every stage of daily lives of the people and telephone tapping is one of such issues. Right to privacy can hardly be claimed or protected in home or office if someone is tapping the conversation on a telephone.<sup>256</sup> Tapping of telephone alia wiretapping<sup>257</sup> has been subjected to attack in recent years and is form of violation of privacy.<sup>258</sup> Like USA telephone tapping or wire tapping poses a serious threat to privacy in India too. Telephone tapping is a gross invasion of privacy unless done for public safety or security of Nation or done in the interest of public.

#### 2.4.4.ii. CCTV: The issue of monitoring

Scholars like Geoffrey Fisher, is of the view that privacy of individual's is an inherent right despite of one's gender. Everyone is entitled to liberty of privacy even before the law.<sup>259</sup> Protection of privacy through law has always invited unavoidable issues. Defining 'privacy' has always been an issue. It is ironic in the sense that at one hand CCTV protects the individuals by tracking the activities of the people (goons) in the sense of public security and on the other hand it intrudes upon the private life of the

---

<sup>256</sup>*Supra* Note at 249.

<sup>257</sup>Wire tapping is a particular form of Electronic Surveillance that monitors telephonic and telegraphic communication. Their introduction of such surveillance raised fundamental issues concerning personal privacy.

<sup>258</sup> Ferdinand J. Jr. Zeni "*Wiretapping-The Right of Privacy versus the Public Interest*" (Volume 40) (Issue 4) (Journal of Criminal Law and Criminology)(Article 5) (J. Crim. L. & Criminology 476 (1949-1950), *available at* <https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=3703&context=jclc> (Last visited on October, 03, 2018).

<sup>259</sup> *Conclusion & Suggestion, available at* [http://shodhganga.inflibnet.ac.in/bitstream/10603/52364/16/16\\_conclusion.pdf](http://shodhganga.inflibnet.ac.in/bitstream/10603/52364/16/16_conclusion.pdf) (Last visited on October 3, 2018).

people. There have been instances where CCTV has infringed the private life of people in hotels etc., which caused mental distress, damage to status and unwelcomed publicity. In such circumstances there arises a conflict between privacy and security. They cannot go in harmony neither be compromised. The right to privacy should not be read only as a private right but should be understood as a right available against the State. The question is not only that of privacy but also of security, and surveillance like that of CCTV in private as well as in public places imposes an overlapping threat.

#### 2.4.5. Issue of Confidentiality in e-Commerce.

Section 72, 72 A of the I.T. Act, 2000 prescribes penal provisions for breach of Confidentiality thereby empowering an aggrieved person to file a suit for compensation before the Adjudicating Authority appointed under Section 46 of I.T. Act, 2000 in a case where a body corporate fails to ensure adoption of reasonable security practices to protect personal data of individuals.

The term ‘Confidentiality’ is related with the prevention of unauthorized information disclosure and its breach on the internet is not difficult and it is the most common issue in e-Commerce.<sup>260</sup>The term confidentiality has also been defined by the “*British Medical Association*”. It mainly dealt with securing the information secure in a secret way from outsiders. Information shared by an individual during his/her career has to be kept secret. Data Protection Act (1998), deals with the legal aspect of preserving confidentiality of UK’s citizen. Regulatory duty is that of processing of information (‘data’) which is identifiable.<sup>261</sup>Internet can no more be considered to be the realm

---

<sup>260</sup> A Sengupta et al, e-Commerce security- A life cycle approach , (Vol.30, parts 2 & 3, April/June 2005, p. 119-140), available at <http://www.ias.ac.in/article/fulltext/sadh/030/02-03/0119-0140> (Last visited on June 22, 2017).

<sup>261</sup>Grant Kelly and Bruce McKenzie, Security, privacy, and confidentiality issues on the Internet (2002),available at <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1761937/> (Last visited on November 18, 17).

<sup>262</sup>of only computer specialists, as the technology has made it available everywhere and for every individuals. The term ‘Confidentiality’ is related with the prevention of unauthorized information disclosure and its breach on the internet is not difficult and it is the most common issue in e-Commerce<sup>263</sup> and by virtue of section 69<sup>264</sup> of the I.T Act 2000, breach of confidentiality has been made punishable.<sup>265</sup> Sensitive personal information, confidential information, or even trade secrets are most often unauthorized collected on the internet leading to its breach and draws awareness from the perspective of invasion of privacy. Generally, all sensitive personal information is regarded to be confidential in nature, but all confidential information may not be regarded only as personal sensitive information as some of them may be of commercial value or interest.<sup>266</sup>

In India the I.T. Act 2000, prescribes punishments with regard to breach of confidentiality under the light of set of Sections whereas, Section 3 of the IT (Reasonable Security Practices and Procedures) Rules 2011 describes the meaning of what sensitive personal information means. As per this Rule of 2011, Sensitive personal information relates to that information consisting of ‘one’s personal information which often consists of sensitive nature and which every individual desires to keep safe. Such information by and large includes password of Bank ATM, Mobile phone etc. and covers details of financial status in bank account and credit

---

<sup>262</sup> Na. Vijayashankar, *Cyber Laws, for every Netizen in India with Information Technology Bill 99* 149, (1<sup>st</sup> Edn. 1999, December), (Publishers, Ujvala Consultants Pvt. Ltd, Bangalore-560050. India.).

<sup>263</sup> A .Sengupta et al, “e-Commerce security- A life cycle approach”, (Vol.30, parts 2 & 3, April/June 2005, pp. 119-140), *available at* <http://www.ias.ac.in/article/fulltext/sadh/030/02-03/0119-0140> ( Last visited on June 22, 2017).

<sup>264</sup> Section 69 of the I.T. (Amended) Act, 2008 prescribes power to issue directions for interception or monitoring or decryption or any information through any computer resources.

<sup>265</sup> Na. Vijayashankar, *Cyber Laws, for every Netizen in India with Information Technology Bill 99* 149, (1<sup>st</sup> Edn. 1999, December), (Publishers, Ujvala Consultants Pvt. Ltd, Bangalore-560050. India.).

<sup>266</sup> Karnika Seth, *Computers, Internet and New Technology Laws* 287-288, A Comprehensive work with a special focus on developments in India, (1<sup>st</sup> Edn.), LexisNexis.

card. In hospitals personal sensitive information includes one's condition of mental health, records etc., and others relates to sexual desires/orientation and information in the form of biometric, which are stored for rendering services by either lawfully or otherwise.<sup>267</sup> Breach of Confidentiality is covered by Sections 72 and 72A, and 43 A of Information Technology Act, 2000<sup>268</sup>, where Section 72<sup>269</sup> of the said Act clearly provides for a statutory right to privacy and confidentiality. It is a significant recognition of a legal framework for Privacy protection. It seeks to punish the non-consensual disclosure to any person of confidential information or such disclosure that compromises the privacy of a data subject. However, this is solely applicable to persons authorised under the Act to secure access to a computer resources. Substantially this section renders greater credence to the law of confidence, route of protection of privacy. It recognizes contractual relations that are based on the overreaching object of confidentiality.

Therefore, the breach of such confidence can be construed as privacy invasion. However, there is no definition provided under the regime for personal information in the Act. Even though the section does criminalize the act of breach of confidentiality, it does not offer any form of compensation to the victim of such breach. In the context of invasion of privacy, that is probably the most important remedy. Therefore, these provisions are not effective means of recourse against intrusion of privacy. By virtue

---

<sup>267</sup> *Supra* Note at 228.

<sup>268</sup> *Supra* Note at 265.

<sup>269</sup>The Information Technology Act, 2000 (Act 21 of 2000), s.72. Breach of confidentiality and privacy.- Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuant of any of the powers conferred under this Act, rules or regulations made there under, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both;

of Section 46 of the I.T. Act 2000, an affected person can sue for compensation before the Adjudicating Authority and remedy is also available in case a body corporate fails to adopt reasonable security practices in protection of personal data of individuals as per Section 43 A of the I.T. Act.

Encryption technologies like “IPS”<sup>270</sup>, “IDS” and “SSL” are among some of the systems which are engaged in preventing, detecting and securing of the data and data base. The issue in these systems is that they only consider data protection and not data privacy. “PPDM” on the other hand is prima facie understood to protect data privacy, but it is not so as it only focus on securing the database owner and not the individual’s in database. <sup>271</sup>

Even the data of a company is protected by the Indian I.T. Act 2000 and its infringement is punishable as per Section 43 and 66. India is a signatory to TRIPS Agreement and therefore protection of trade secrets is protected by virtue of Article 39 of the agreement, and in case of breach of any confidential information, an action for breach of confidence and payment of damages can be filed by lodging a suit for injunction and compensation. Any Confidential Information also finds place under the Copyright Law and Common Law. Some jurisdiction have their separate legislation to protect Confidential Information or Trade Secrets while in India this two are protected by contract law or by the law of torts,<sup>272</sup> and any disclosure of

---

<sup>271</sup> “IPS” stands for Intrusion Prevention, “IDS” for Intrusion Detection, “SSL” for Secure Data Layer and “PPDM” for Privacy-Preserving Data Mining.

Stephen E. Fienberg “Privacy and Confidentiality in an e-Commerce World: Data Mining, Data Ware Housing, Matching and Disclosure Limitation” (11 Sep.2006), *available at* <https://arxiv.org/pdf/math/0609288.pdf> (Last visited on August 13, 2018).

<sup>272</sup> Karnika Seth, *Computers, Internet and New Technology Laws, A Comprehensive work with a special focus on developments in India* 281 (1<sup>st</sup> Edn.), Lexis Nexis.



information to another party in confidence is protected by the law of torts and by the principles of equality which disallows a person to take unfair advantage of information granted or disclosed to another in good faith and confidence. Therefore disclosure of any confidential information of a person to whom such information belongs without due permission leads to its infringement.

#### 2.4.5.i. Exception to Breach of Confidence

Public interest, law enforcement needs, national security, public record, breach of law, statutory duty and fraud are some of the few exceptions that lies to breach of confidence. A disclosure of confidential information to law and enforcement authorities is not considered to be actionable. In case of *Onkar Lal Bajaj v Union of India*,<sup>273</sup> the Supreme Court of India took into consideration the term ‘public interest’/ ‘probity in governance’ and observed that it cannot be narrowly or strictly interpreted, and its interpretation solely depends on circumstances of each case. The I.T. Act, 2000 also prescribes certain exception regarding disclosure of confidential information in National interest. Though government agencies are barred from disclosing or publishing or sharing such information with any other person, Sections 69 and 69 B grants special power to the Central Government regarding authorization and monitoring of information’s to ensure security and no legal obligation is required to be complied with for taking of prior permission from the provider.<sup>274</sup>

#### 2.4.5.ii. Ingredients of Confidential Information

Information of confidential nature holds four basic requirements. The first thing to be considered is that the information should be of such nature as its disclosure to

---

<sup>273</sup> (2003) 2 SCC 673, AIR 2003 SC 2562

<sup>274</sup> *Supra* Note 274 at 291

competitors may cause damage to its owner. Secondly, the confidentiality of the information should be trusted by its owner and thirdly, the confidentiality of the information should be reasonable, and lastly, the confidentiality of the information must be considered with regard to the industry practices specified to each industry.<sup>275</sup>

In determining the confidentiality of information several other factors are also taken into considerations<sup>276</sup> which are as follows: -

- The extent to which such information is known to business firms apart from the owner.
- The extent to which such information is known to the employees.
- Steps take to preserve its secrecy
- Value that lies in the information to the owner and his competitors.
- The amount of money spent in creating the information.
- The ease with which such information can be required or copied by others by their individual efforts.<sup>277</sup>

#### 2.4.5.iii. Obligations of Confidentiality-Expressed and Implied

In a contract there is an offer and acceptance and parties sign their terms where one party may have disclosed some confidential information to another for the purpose of the performance of the contract. There is an implied obligation posed by the law in regard of dealing with the confidential information with copious caution. This obligation persists in the absence of expressed clause which deals with safeguarding of confidential information. In case of absence of a specific legislation to deal with

---

<sup>275</sup>*Supra* Note at 268.

<sup>276</sup>*Supra* Note at 273.

<sup>277</sup>*Supra* Note at 273.

matter of protection of trade secrets, like confidential information, trade secrets will also be protected by the law of contract or by the law of torts, in India. To bring action for breach of confidentiality, the burden of proof falls on the plaintiff to furnish that the information is of confidential nature along with the implication of it being a secret.<sup>278</sup>

#### 2.4.5.iv. Remedies under Common Law for Breach of Confidentiality

Common law as applicable in country like Britain is also applicable in India and legal remedy is reachable for any action for breach of confidentiality by grant of injunction order which may be temporary or permanent one, whenever applicable damages and delivery up of confidential information is also available. The grant of injunction by the Court depends on the nature of the confidentiality, and is granted accordingly viz, temporary injunction is granted if the information is confidential, only for a stipulated period of time and thus a balance of convenience are reached by the court while granting of injunction to parties. The court further takes into account other things such as the effect of injunction, its harmfulness on the defendant, and ambiguous nature of the injunction insisted upon. While granting compensation market value of the confidential information or injury caused to an individual is accessed by the court.<sup>279</sup>

#### 2.4.6. Issues in Social Networking Messaging Sites

Social networking sites include domains like WhatsApp, Facebook, Google, Tweeter, MySpace etc. Huge quantum of personal information is shared by the users in Online Social Networks (OSNs) and leads to issues of privacy, data privacy, data theft and

---

<sup>278</sup> Karnika Seth, *Computers, Internet and New Technology Laws, A Comprehensive work with a special focus on developments in India* 290 (1<sup>st</sup> Edn.), LexisNexis.

<sup>279</sup>*Id.*

sensitive Data.<sup>280</sup> Every time the user is engaged in an online activity, their privacy is intruded without the knowledge and their consent. Users shares different shades of information ranging from personally identifiable information to sensitive information which are replicated in several occasions to the third parties for commercial gains.<sup>281</sup> Web 2.0<sup>282</sup> has enabled Social Profiling and has raised growing concern for internet privacy by facilitating Participatory Information Sharing and Collaboration. Facebook and MySpace are an example of Web 2. With the growth of technology and advancement of cloud computing people started sharing their personal information. These social networks<sup>283</sup> keep a track of all the interactions used on their sites. The information so tracked are saved for later use and attracts problems like cyber stalking, social profiling, location disclosure, third party information disclosure and Government use of information for investigation without the safeguard of search warrant.<sup>284</sup> The volume and accessibility of information on social media sites attracts malicious people who seek to exploit this information. A common social networking risk includes Spear phishing, social engineering, and spoofing. Security and privacy related to social networking are fundamentally behavioral issues not technology issue. The more information a person posts the more information is available for potential compromise.

---

<sup>280</sup> Agrima Shrivastava “Enhancing Privacy in Online Social Networks using Data Analysis” (2015), available at <http://shodhganga.inflibnet.ac.in/bitstream/10603/125427/1/synopsis.pdf> (Last visited on August 13, 2018).

<sup>281</sup> Sabine Trepte and Leonard Reinecke “The Social Web as a Shelter for Privacy and Authentic living”, available at <https://pdfs.semanticscholar.org/b526/5e67813a5b1440c4d61a311e62a4c3328a1f.pdf> (Last visited on August 13, 2018).

<sup>282</sup> *Web 2.0*, also called Participative (or Participatory) and *Social Web*, refers to World Wide *Web* websites that emphasize user-generated content, usability (ease of use, even by non-experts), and interoperability (this means that a website can work well with other products, systems, and devices) for end users.

<sup>283</sup> Social Networking Sites have become very popular avenues for people to communicate with family, friends, and colleagues from around the corner across the Globe.

<sup>284</sup> Social Networking Sites privacy issues overview, (Handson ERP) (Published on Jan 8, 2014), available at <https://www.youtube.com/watch?v=EGIAbmTwmvk> (Last visited on August 13, 2018).

#### 2.4.6.i. Facebook

Privacy has been infringed on many social networking messaging sites like Facebook, WhatsApp and Tweeter. Among them Facebook is the best example so far. Kalev Leetaru, one of the contributors at Forbes, American business magazine, on March 23, 2018, at 1:52 pm had expressed his view on the impact of Facebook on privacy. He stated that, “*Facebook succeeded in killing cybersecurity like it did privacy*”.<sup>285</sup> He further went to state that, the relevance of privacy in this modern age has been outdated by the use of Facebook, as people share their intimate details to private company to commercialize and users even don’t care that their data are being misused by the company world-over without their consent.<sup>286</sup>

The issue of privacy, data and cybersecurity are being accelerated by the Facebook users as they voluntary provide their password, and other personal details to Facebook employee. No matter how their personal information’s are traded by these employees, people are not going to stop using Facebook. The importance of privacy, security and data will soon become a myth if people don’t stop acting blindfolded to the menace done by these social networking messaging sites. The most relatable question asked today is “Is WhatsApp safe?” WhatsApp is a Facebook-owned messaging platform estimated to be used by one billion people.<sup>287</sup>

---

<sup>285</sup> Forbes, *available at* <https://www.forbes.com/sites/kalevleetaru/2019/03/23/facebook-succeeded-in-killing-cybersecurity-like-it-did-privacy/#52e30db84549> (Last visited on January 16, 2020).

<sup>286</sup>*Supra* Note at 282.

<sup>287</sup>James Frew, Security Threats Users Need to Know About, (Updated on December 17, 2019), *available at* <https://www.makeuseof.com/tag/4-security-threats-whatsapp-users-need-know/> (Last visited on January, 16, 2020).

#### 2.4.6.ii. E-Mail, Press & E-Mail Misuse

Emails<sup>288</sup> have become an even more shared tool to communicate. Email accounts usually are hacked to access the personal, sensitive, or confidential information that they might contain. It damages personal information relating to one's bank account and profiles too including websites.<sup>289</sup> Like Facebook, it too contains the information of people and those information's are either personal and of sensitive nature.

### 2.5. Conclusion

Different genres of Privacy and Data Protection issues have been tracked down in this chapter. This chapter focused on the two different issues in e-Commerce i.e. Legal and Techno-legal issues of privacy and data protection. The advancement in technology and online platform beyond one's control and unlimited nature of jurisdiction made a gateway to unstoppable cyber crimes which are difficult to curb down in the absence of effective laws. Though a new beam of hope is drawn by the Data Protection Bill and Consumer Protection Bill, 2018, our people, legal and regulatory authorities are still praying to see the actual light. Our laws have proven again and again to be inefficient in front of the giant technology which is targeting consumer's data and privacy at an alarming speed. Consumers are victims of technological advancement and online transactions which takes place at anytime and anywhere. In the absence of laws on Data Protection, it becomes very suffocating to safeguard one's privacy and data. The problem is more severe when data is

---

<sup>288</sup>Email is a widely used communication mechanism that can be categorized into two basic types of web-based service: open and closed. Open web-based services provide email accounts to anyone, either for free or for a fee. Closed web-based services are managed by organizations who provide email accounts only to their members. Email is used by commercial and social websites because of its security.

<sup>289</sup>Hacking, *available at* [https://en.wikipedia.org/wiki/Email\\_hacking](https://en.wikipedia.org/wiki/Email_hacking) (Last visited on August 10, 2018).

transferred from one jurisdiction to another without obtaining prior permission or knowledge of data subjects.

## CHAPTER THREE

### LEGAL FRAMEWORK FOR PRIVACY & DATA PROTECTION IN e-COMMERCE AND INTERNATIONAL DOCUMENTS

#### 3.1. Introduction

Immanuel Kant, a prominent German Philosopher (1724-1804), has identified the importance of right and dignity in one's life. He opines that "*humanity itself is a dignity*"<sup>290</sup>, and one needs to be respected by another individual. Every facet of human life and human behavior is said to be in relation to the law.<sup>291</sup> Privacy is another aspect which forms an integral part of every individual and is in a constant attention of being protected from the monsters of today's technology. Privacy is not borrowed but inherent since the time immemorial; its value can be traced back to the Biblical period supra. <sup>292</sup> The theory of privacy can be understood as the right free from intrusion. The importance of privacy is so much so that it has successfully tattooed its place in almost all international human rights documents<sup>293</sup>. Countries like USA and India have recognized this right through case laws<sup>294</sup>. The issue in

---

<sup>290</sup> Rowan Cruft, S. Mathew, *et.al.* (eds.), *Philosophical Foundations of Human Rights*.

<sup>291</sup> E.J. Jathin "Human Genome Project: Emerging Challenges of Right to Privacy vis-à-vis Insurer's Right to Know" 2 (Vol. XXXI) (March-June) *C.U.L.R.* (Number 1&2) (D. Rajeev Edtr.),(N.S. Gopalkrishnan & A.M. Varkey (eds.) (2007).

<sup>292</sup> *Supra* Note at 284.

<sup>293</sup> Universal declaration of Human Rights 1948, art.12, International Convention on Civil and Political Rights-1966, art.17, European Convention of Human Rights-1950, art.8, American Convention on Human Rights-1969, art.111, African Charter on Human Rights and Welfare of Child-1990, art. 10, Cairo Declaration of Human Rights in Islam-1990, art. 18(b), Arab Charter on Human Rights 1994, art.17.

<sup>294</sup> Indian Constitution for the first time in *J. Puttaswamy* case discussed on different facets of privacy. Earlier the Supreme Court in *Kharak Singh v. State of Uttar Pradesh*, (A.I.R. 1963 S.C. 1295) recognized this right as implicit in *art. 21* by expanding *right to life and personal liberty*, to include right to privacy. In United States, Supreme Court recognized this right in *Roe v Wade* [410 U.S. 113 (1973)] as a part of personal autonomy of the individual. Court also mentioned that the roots of that



protection of right to privacy is regarding how far this right can be protected as against the other person's right? Privacy has a more difficult path to go through when it enters the world of e-Commerce. E-users need to have a certain level of trust and confidence while transacting online or when engaged in e-Commerce as they are not only purchasing but are risking their privacy and valuable data<sup>295</sup>. Individual demands security while purchasing online. They want to keep their interest and preferences private and unknown to the world. This need of seclusion raises legal issues of privacy and security. This legal issue is not limited to commerce only but extends to other general use of the internet. People believe that their activities on internet are private, free from intrusion and safe from being hacked. The idea owes to the fact that they rarely provide their personal information and if they provide they are convinced by the privacy or security guarantee norm provided at the website page. Their idea is misplaced as there are many mechanisms that collect information regarding surfers like, goods purchased, sites visited, personal information, and so on. The need to protect data and data privacy in India is relatively new and Indian legal framework for protection of data is warranted under the current circumstances and in incidents of data theft and breach of data privacy. India cannot ignore data security issues for much longer so as so it continues to be a hotspot for off-shoring<sup>296</sup>.

---

right can be found in the concept of liberty guaranteed in the Constitution through fourteenth amendment.

<sup>295</sup> While engaging in e-Commerce almost every e-user are aware of the fact and danger in using credit card numbers as there is a fear of its disclosure to the whole world. Such dangers are posed by hackers etc. In such unguarded security level, fear over one's privacy is common, Ramnath K. Chellappa, "Consumer's Trust in Electronic Commerce Transactions: The Role of Perceived Privacy and Perceived Security", available at <https://pdfs.semanticscholar.org/7e2f/bad4fa4877ea3fd8d197950e335d59ebedf.pdf> (Last visited on September 8, 2018).

<sup>296</sup> Latha R. Nair, "Data Protection efforts in India: Blind Leading the Blind?" 2 (*NLSIU India Journal of Law and Technology*) (Westlaw India) (2008).

### 3.2. Legal Framework for Privacy –Indian scenario

In the legal framework Indian laws are discussed. Altogether eight laws are discussed below, which includes the Constitution of India, Jurisprudence Law, Law of Tort, Information Technology Act, 2000, Information Technology (Amended) Act, 2008, The Consumer Protection Act, 1986, Security Exchange Board of India (SEBI) and Reserve Bank of India (R.B.I).

#### 3.2 i. Privacy under the Constitution of India

The concept of privacy though not defined in the ancient times holds an old idea<sup>297</sup>, and traditional society had also valued it to some extent<sup>298</sup> but due to the absence of internet and technology, the need for providing legal protection and legislation for the same was not deeply felt. But early society did felt insecure about their “*honor* and reputation”.<sup>299</sup> A movement for the development for the protection of privacy was not limited to India<sup>300</sup> but was also initiated in the countries like U.S.A.<sup>301</sup> and

---

<sup>297</sup>BP Dwivedi “Emerging Right to Privacy an Indian Perspective” “Conceptual and Constitutional Foundation”, *available at* [http://shodhganga.inflibnet.ac.in/bitstream/10603/137097/7/07\\_chapter\\_02.pdf](http://shodhganga.inflibnet.ac.in/bitstream/10603/137097/7/07_chapter_02.pdf) (Last visited on September 4, 2018).

<sup>298</sup>*Id.*

<sup>299</sup>Barkha and U. Rama Mohan, *Cyber Law & Crimes 165* (Published by S.P. GOGIA, H.U.F.) (2013).

<sup>300</sup>Traces of our Indian history makes it clear that privacy of an individual especially of women were kept at priority list. It included personal sensitive information like family and procreation. Duty of States to protect the privacy of Citizens was also seen to be written in ‘Dharmashastras’. Principle of ‘non-interference’ is not new, as it was developed as early as in the reign of Kings. Our Constitution of India did not directly talked about the right to privacy although, interests similar to that have been protected both under civil law and under the Penal Code, the Evidence Act and under the Constitution, LawRelating to Right to Privacy in India – An Analysis, *available at* [https://shodhganga.inflibnet.ac.in/bitstream/10603/98806/11/11\\_chapter%204.pdf](https://shodhganga.inflibnet.ac.in/bitstream/10603/98806/11/11_chapter%204.pdf) (Last visited on June, 17, 2018).

<sup>301</sup>*Griswold v. State of Connecticut*, 1965 SCC OnLine US SC 124, In this Case in para 32 the Court stated that.-

Privacy must come under “fundamental rights” and every country should make provisions for the same in their “Constitution”. *Olmstead v. United States* is another important case which summarized the principles underlying the Constitution's guarantees of privacy, *available at* <https://www.sconline.com/Members/NoteView2014.aspx?citation=JTXT-0000431222&&&&&40&&&&&Search&&&&&fullscreen> (Last visited on August 19, 2018).

U.K.<sup>302</sup>This right is often expressed as the right against the whole world<sup>303</sup>. No such right as ‘right to privacy’ was recognized under the Indian Constitution. It was only skewed and sifted through various judgments of the Apex court<sup>304</sup>.

The term privacy and confidentiality<sup>305</sup> are now used synonymously. The issue of confidentiality is a new concept and got recognition only when it was read at par with privacy. <sup>306</sup>Personal Information identifies an individual and is not limited to the person’s name, date of birth, marital status, contact information, ID issue and expiry date, financial records, credit information, medical history, where one travels, and intentions to acquire goods and services.<sup>307</sup>

---

<sup>302</sup> Right to Privacy was also recognized in U.K. and it is evident from the introduction of ‘House of Commons Bill’ on November 26<sup>th</sup> of 1969. This Bill was introduced by the then MP Mr. Brian Walden. Other former Bills include Bills of 1961 and 1967. The U.K. Government also took initiative on ‘privacy’ protection and stated that legislation must be strengthened to provide complete privacy protections to individuals and consumers per se, Importance of Right to be ‘left alone’ and ‘Anxiety over privacy’ were also instituted in UK. ‘Anxiety UK’ is another important aspect in UK, which ensures and respect privacy of an individual, *available at* <https://www.anxietyuk.org.uk/privacy-policy/> (Last visited on October 19, 2018).

<sup>303</sup> Arun Mal & Jenisha Parikh, “Facebook and Right to Privacy: Walking a Tight Rope” (2011) 4 *NUJS L Rev* 299, *available at* <https://www.sconline.com/Members/NoteView2014.aspx?citation=JTXT-0000003719&&&&40&&&&Search&&&&fullscreen> (Last visited on October 19, 2018).

<sup>304</sup>Ms. Talat Fatima, “Privacy on the Web” 23 (Vol.1) 2005 *CLC1 (Mad) CLC 273 (Delhi)* (Shri D. Varadarajan Edtr.)(2005).

<sup>305</sup> The term Confidentiality involves both expressed and implied principles of confidence upon a person other than self. The concept of privacy is very relevant and incurs implied obligation and is related to the concept of confidence as in both the case individual claims on, how their information is communicated to others, *available at* <http://www.legalserviceindia.com/article/1413-Breach-Of-Confidentiality-&-Various-Legal-Issues.html> (Last visited on October 21, 2018).

<sup>306</sup> Duty of data subject to have confidence confers the right over information which cannot be used or disclosed for purposes not given consent for, Vibhor Verdhan “Breach of Confidentiality and Various Legal issues”, *available at* <http://www.legalserviceindia.com/article/1413-Breach-Of-Confidentiality-&-Various-Legal-Issues.html> (Last visited on October 19, 2018).

<sup>307</sup>Legal Service India- Breach of Privacy and Confidentiality under Information Technology Act, 2000, *available at* <http://www.legalserviceindia.com/article/1288-Breach-of-privacy-&-Confidentiality-.html> (Last visited on August 23, 2018).

The entire issue was on the constitutionality of the right to privacy, the right necessarily subservient to the national interest<sup>308</sup>. *Puttaswami case supra*<sup>309</sup> is the latest achievement in acknowledging privacy as a right under article 21. Cases like *Kesavananda*, AIR 1973 SC 1461 have been discussed in the opening chapters supra 1 and 2, concerning the concept of privacy. Article 21<sup>310</sup> is the source for every reader's to peruse and connect the landmark judgments to understand the concept of privacy in Indian society. The principles of freedom of speech<sup>311</sup> are found in many international documents and Constitutions and are simply an articulation and are liberally exercised by the people after the judgment came in *Shreya Singhal v Union of India*.<sup>312</sup>In order words freedom of speech<sup>313</sup> is the idea of expressing views without the fear of harassment.<sup>314</sup> People over the years have understood the nexus between Arts. 19(1) (a)<sup>315</sup> and 21<sup>316</sup> of the Constitution of India and some of the authors have expressed it as those rights which cannot be exercised in the absence of another.<sup>317</sup> The term privacy<sup>318</sup> is approached differently by each individual's. Such difference in approach is because of the society, one is subjected to. Breckendridge in his book "The Right to Privacy, 1971", described privacy as a right where only the

---

<sup>308</sup> The Constitution of India.

<sup>309</sup> (2017) 10 SCC 1.

<sup>310</sup> The Constitution of India.

<sup>311</sup> *Id.*

<sup>312</sup> (2015) 5 SCC 1

<sup>313</sup> Freedom of speech has also been defined under judicial lexical as a right to express against own government. It implies that the subject won't be punished for expressing his/her opinion. Rick Falkvinge "You don't have freedom of speech without privacy" (2016), *available at* <https://www.privateinternetaccess.com/blog/2016/08/dont-freedom-speech-without-privacy/> (Last visited on September 5, 2018).

<sup>314</sup> *Id.*

<sup>315</sup> "Freedom of speech and expression"

<sup>316</sup> "Protection of life and personal liberty"

<sup>317</sup> Rick Falkvinge, Privacy News Online, *available at* <https://www.privateinternetaccess.com/blog/2016/08/dont-freedom-speech-without-privacy/> (Last visited on February, 17, 2018).

<sup>318</sup> The term 'Privacy' has also been divided into three strata, i.e., by physical space, by choice and by information which are personal, *available at* <https://www.ntia.doc.gov/legacy/ntiahome/privacy/files/CPRIVACY.PDF> (Last visited on September 5, 2018).

owner of the information shall have control over deciding on which part shall be private and which shall be available for public. In other words it meant that only the owner shall have full control over the information.<sup>319</sup>

Aadhaar case supra<sup>320</sup> is the finest case on right to Privacy in India till date. It prima facie appeared to be the most undecided genre of the said issue before the Bench comprising of three Judges deciding the validity of the Aadhaar. It became inevitable to settle on this issue of privacy before deciding the matter of Aadhaar. Hence the question was referred to Chief Justice of India to be put before a Bench of five judges of the Supreme Court which ended up into formulation of a Bench of nine judges for the settlement of the uncertainty over the essence of Right to Privacy.<sup>321</sup> As stated earlier in the previous chapters this right is now a fundamental right under article 21 of the Indian Constitution.

The State has a concomitant obligation to define as well as protect data and privacy.<sup>322</sup> Protection of data will not only protect the privacy but will also help in safeguarding the autonomy of individuals. Right to privacy is now part of the Fundamental right by the effort brought in the landmark case of *Puttaswamy* supra. The judgment subconsciously emphasizes on the need of having a data protection law

---

<sup>319</sup>Madhavi Divan, “The right to privacy in the age of Information and Communication”, (2002) 4 SCC J-12, *available at* <https://www.sconline.com/Members/SearchResult.aspx> (Last visited on February 21, 2020).

<sup>320</sup>*Binoy Visman vs Union of India*, (2017) 7 SCC 1

<sup>321</sup> The Court in *Puttaswamy* case not only attempted to define the nebulous concept of ‘privacy’ but did analyzed the various hues and shades of ‘privacy’ and finally contained the myriad concept of ‘privacy’ within perceptible contours, *available at* <https://medium.com/indrastra/an-analysis-of-puttaswamy-the-supreme-courts-privacy-verdict-53d97d0b3fc6> (Last visited on December 19, 2018).

<sup>322</sup>Dr. R. Venkata Rao & Dr. T.V. Subba Rao (eds.) “A Public Discourse on Privacy-An Analysis of Justice K.S. Puttaswamy v Union of India” 52 (Foreword by Hon’ble Justice Prof. Dr. S. Rajendra Babu).

and highlights the principle of consent and informational privacy in the era of big brother trend.

### 3.2. ii. Jurisprudential aspect of Privacy

The juridical vision of right to privacy implies the right as not merely to prevent incorrect description of private life but the right to prevent its being depicted at all<sup>323</sup>. Judiciaries have always tried to protect privacy of individual's, by interpreting Article 19 and 21 of the Indian Constitution. Evidence is in the form of various landmark pronouncements supra. On various occasions this right was debated to be exclusionary from fundamental rights. *A.K. Goplalan* supra<sup>324</sup> marked those fundamental rights as emblazoned in the Constitution as "isolated silos"<sup>325</sup>, whereas, in *M.P. Sharma* supra, to be not an authority for deciding the absence of right to privacy under the Indian Constitution. The State has a concomitant obligation to define as well as protect data and privacy.<sup>326</sup> Protection of Data will not only protect the privacy but will also help in safeguarding the autonomy of individuals. The landmark judgments in the face of *MP Sharma*<sup>327</sup> and *Kharak Singh*<sup>328</sup> supra failed to bring into purview the definition of privacy and did not gave a place in the pigeon hole of Fundamental rights enshrined in the Constitution of India. Today, privacy as a right has gained momentum and is one of the best decisions of constitutional bench.

---

<sup>323</sup> Raghavendra Kumar, "Right to Privacy: Juridicial Vision" 195 A.I.R. (Vol.89) (RAJ.SIK) (Acts N.O.C.) (Published by: S.W. Chitale for All India Report Pvt. Ltd.) (Printed at the Air Rotary Printing Press) (2002).

<sup>324</sup> *A K Gopalan v State of Tamil Nadu*, AIR 1950 SC 27

<sup>325</sup> In 1924 and 1962, when the Supreme Court's eight-and six-judge benches decided the cases of *M.P. Sahrma v Sagtish Chandra*, District Magistrate, Delhi and *Kharak Singh v State of Uttar Pradesh* respectively, the court was equipped with the 1950 *A K Gopalan v State of Madras* for a precedent. Article 19, guaranteeing a certain freedom was held exclusionary from Article 21, guaranteeing life and personal liberty, available at <https://www.livemint.com/Politics/7oHGx6UJfLD0uIDXFwV9CL/Is-privacy-a-fundamental-right-Two-cases-that-Supreme-Court.html> (Last visited on December 19, 2018).

<sup>326</sup>Dr. R. Venkata Rao & Dr. T.V. Subba Rao (eds.) "A Public Discourse on Privacy-An Analysis of Justice K.S. Puttaswamy v Union of India" 52.

<sup>327</sup>*MP Sharma v Satish Chandra* (1954)

<sup>328</sup>*Kharak Singh v State of Uttar Pradesh* (1962)

Right to privacy is now part of the Fundamental right by the effort brought in the number of landmark cases as stated before time and again.

The active role of judiciary has been successful in recognizing right to privacy as an essential ingredient of right to life and personal liberty<sup>329</sup>. Apex courts has interpreted privacy in various judgments and have defined it as a desire to be left alone, the desire to be paid for one's data and ability to act freely<sup>330</sup>. The right to privacy in India is a blend of constitutional, customary and common law rights stretched across various legal field. Despite of multiple reasons for a strong and comprehensive need for data Protection law, India lacks a positive willingness to adopt data privacy laws. For many years India has been flooded with questions regarding whether a 'right to privacy' exists in e-Commerce? There is still an ongoing debate on the uncertainty about conceptual basis of privacy and data privacy laws<sup>331</sup>.

### **3.2.iii. Privacy under law of Tort**

Indian Law of tort has been influenced by the Law of Torts of England and is commonly known as the Law of Tort. As per this law, protection of data will not only protect the privacy but will also help in safeguarding the autonomy of individuals. As stated earlier, number of landmark judgments <sup>332</sup> had failed to bring into purview the definition of privacy and did not gave it a place in our Constitution. Law of Tort treats violation of privacy as defamation and as an offence under section 499 of the Indian

---

<sup>329</sup>*Govind v State of MP* (1975)

<sup>330</sup> Shiv Shankar Singh, "Privacy and Data Protection in India: A Critical Assessment", *Journal of Indian Law Institute* 665(Volume 53) (October-December) (Westlaw India) (Number 4) (2011).

<sup>331</sup>Subhajit Basu, "Policy-Making, Technology and Privacy in India"<sup>7</sup> (NLSIU Bangalore) *Indian Journal of Law and Technology* (2010).

<sup>332</sup>*MP Sharma v. Satish Chandra* (1954)

Penal Code<sup>333</sup>. Similarly section 72 of the Information Technology Act, 2000 regarded its violation as an offence<sup>334</sup>.

### **3.2.iv. Privacy under the Information Technology Act, 2000**

Before outlining the Information Technology Act in the genre of privacy and data protection, it may be noted down that India have a hub of Laws dealing with the data protection, but none of them stands satisfactory in solving the tricky issues laid down by the web networks. These laws are divided considering the different sectors such as, Finance, Health, Information Technology and Telecommunications and lastly miscellaneous covering the latest ‘White Paper’ on data protection framework for India<sup>335</sup>.

The Information Technology Act, 2000 (21 of 2000), walks on the footsteps of “UNCITRAL Model Law”. The Act has recognised “e-Commerce”, and has included penalty provisions to issues in connection to it. It can be reiterated that this Act has modified sections of other Acts to offer a balance in the contemporary internet age. The saga of traditional contract has been replaced with the modern e-Contract and has changed the way of conducting business. The new form of commerce is cost effective as well as time effective. This internet age has invited issues and therefore this Act has incorporated liability provisions i.e. Civil and Criminal.

---

<sup>333</sup>Ms. Talat Fatima, “Privacy on the Web” 23(Vol.1) 2005 *CLCI (Mad) 2005 CLC 273 (Delhi)*, Shri D. Varadarajan (Edtr.) (2005).

<sup>334</sup> Section 72 of the Information Technology Act, 2000 (Act 21 of 2000) entails two aspects of the offence. The first one restricts access to others personal information with obtaining the consent and the second one restricts its disclosure to third parties, *available at* <https://privacyinternational.org/state-privacy/1002/state-privacy-india> (Last visited on July 25, 2020).

Ms. Talat Fatima, “Privacy on the Web” 23 (Vol.1) 2005 *CLCI (Mad) 2005 CLC 273 (Delhi)*, Shri D. Varadarajan (edtr.)(2005).

<sup>335</sup> Indian Laws dealing with Data Protection, *available at* <http://vikaspedia.in/e-governance/national-e-governance-plan/data-privacy-and-protection/indian-laws-dealing-with-data-protection> (Last visited on August 8, 2018).



The Indian Penal Code which was enacted back in 1860 dealt with the cyber offences until the introduction of the I.T. Act, 2000. India does not have any laws to deal specifically with the issues in e-Commerce; therefore, Legislators modified the provisions of the pre-existing laws<sup>336</sup> to address issues which are not dealt by the I.T. Act.

Within a couple of years of the birth of I.T. Act, 2000, technology started to dominate the society. Crimes are committed via computer by the people belonging to different age groups with the help of internet.<sup>337</sup> A new dominating act was indeed needed to curb out the menace by insertion of new kinds of cyber offences and to strengthen the I.T. Act, supra.<sup>338</sup>

In recent years internet has brought the whole world closer by turning it into a global village alias cyberspace which has now turned out to be a niche for new risks threatening one's privacy and with the advent of information technology people's interest in protecting the same has been increased over the years.<sup>339</sup> The dawn of technology has forced to give prominence to data and information. The increasing human interaction on an online platform is one of the concerns to be addressed regarding privacy and data protection. With the generation of data in an online space, added with its vulnerability of being misused, is posing a threat as well as challenge to our present legal and regulatory framework. The violation of privacy is further

---

<sup>336</sup> "Indian Penal Code", "Indian Evidence Act"

<sup>337</sup> Available at [https://en.wikipedia.org/wiki/Surface\\_computer](https://en.wikipedia.org/wiki/Surface_computer) (Last visited on December 21, 2018).

<sup>338</sup>S. Praveen Raj et al. "Comparison between Information Technology Act, 2000 & 2008", "International Journal of Pure and Applied Mathematics" (Vol. 119, No. 17) (2018), available at <https://acadpubl.eu/hub/2018-119-17/2/141.pdf> (Last visited on March 18, 2019).

<sup>339</sup>S.K. Verma & Raman Mittal (eds.) "Legal Dimensions of Cyberspaces".

activated with the accumulation of considerable amount of data on internet which is easily accessible to anyone. In such kind of unavoidable circumstances, the need for privacy protection cannot be underrated.<sup>340</sup>

E-Commerce has been given a legal sanction by the Information Technology Act of 2000. There exists grey areas in its provisions and it would not be wrong to point out that this Act has failed to protect the privacy and data privacy of people.<sup>341</sup> Privacy is also understood the wholesome right a person to exercise restraint on information about him. While some author defines privacy as keeping one's information secret from the other fellow beings.<sup>342</sup> Hence, some conclude that the concept of privacy is used to describe not only rights purely in the private domain between individuals but also constitutional rights against the State.<sup>343</sup> Under the I.T. Act, 2000 there is no provision for data protection. There is an inherent conflict between right to privacy and data protection.<sup>344</sup> The mushrooming of technologies has spawned a different set of issues concerning privacy rights and data protection.<sup>345</sup> In order to resolve conflicting issues inherent in the interests to information, data protection should come

---

<sup>340</sup>*Supra* Note at 330.

<sup>341</sup>Paven Duggal, (2000), available at <http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan002090.pdf> (Last visited on June 22, 2017).

<sup>342</sup> Privacy, available at [https://www.huffpost.com/entry/having-privacy-vs-keeping\\_b\\_9242666](https://www.huffpost.com/entry/having-privacy-vs-keeping_b_9242666) (Last visited on June 22, 2017).

<sup>343</sup>Raman Mittal & Neelotpal Deka, *Cyber Privacy, Legal Dimensions of Cyberspace* 198(S.K. Verma & Raman Mittal (eds.), (ILI, India).

<sup>344</sup> The data protection may include financial details, health information, business proposals, intellectual property and sensitive data. Data Protection and privacy have been dealt within the Information Technology (Amended) Act, 2008 but not in an exhaustive manner. The Act is not sufficient in protection of data and hence a separate legislation in this regard is required, Vijoy Dal Dalmia, "India: Data Protection Laws in India-Every Thing You Must Know" (Last updated: 13 Dec. 2017), available at <http://www.mondaq.com/india/x/655034/data+protection/Data+Protection+Laws+in+India> (Last visited on January 12, 2019).

<sup>345</sup> Shiv Shankar Singh, "Privacy and data Protection in India: A Critical Assessment" 663 *JL of THE INDIAN LAW INSTITUTE* (Vol. 53, 1-4, 2011) (July to September 2011) 53 *JILI* (2011) (2011).

into play and protect individuals and organisations in such a manner that their privacy rights are not compromised.<sup>346</sup>

The absorption of internet in our lives has become extraordinary. There are ample of examples relating to our reliance on internet and computer in all facets of lives.<sup>347</sup> I.T. Act has been said to be stalked by the constant fear of invasion of privacy owing to massive potential of modern technology and its associated systems like internet to creep into personal information.<sup>348</sup>

Chapter IX and X of the I.T. Act 2000, deals with sections regarding offences and punishments. Section 43<sup>349</sup>, 44<sup>350</sup>, 65<sup>351</sup>, 66<sup>352</sup>, 68<sup>353</sup>, 70<sup>354</sup>, 73<sup>355</sup>, 74<sup>356</sup>, 77-A<sup>357</sup> checks and punishes the offenders.

### **3.2. v. Privacy under the Information Technology (Amended) Act, 2008**

The Information Technology Act, 2000 as discussed above did not specifically provided protection of sensitive personal data.<sup>358</sup> The Indian Act which addresses the

---

<sup>346</sup>*Supra* Note at 337.

<sup>347</sup>Desai, Prashant S,” Legal protection of right to privacy in the era of information technology a critique” “Information Technology and Threat to Privacy -An Analysis”, *available at* [http://shodhganga.inflibnet.ac.in/bitstream/10603/98806/13/13\\_chapter%206.pdf](http://shodhganga.inflibnet.ac.in/bitstream/10603/98806/13/13_chapter%206.pdf) (Last visited on August 31, 2018).

<sup>348</sup>Aravind Menon *THE eLAWS* 359 (Forwarded by Hon’ble Mr. Justice K.T. Thomas) (1<sup>st</sup> Edn. 2011).

<sup>349</sup>“Penalty and Compensation for damage to computer, computer system, etc.”

<sup>350</sup>“Penalty for failure to furnish information, return, etc.”

<sup>351</sup>“ Tampering with computer source documents”

<sup>352</sup>“Computer related offences”.

<sup>353</sup>“ Power of Controller to give directions”

<sup>354</sup>“Protected system”

<sup>355</sup>“Penalty for publishing electronic Signature Certificate false in certain particulars”

<sup>356</sup>“Publication for fraudulent purpose”

<sup>357</sup>“Compounding of offences”

<sup>358</sup> “The Indian Ministry of Information Technology and the National Association of Software and Service Companies (NASSCOM) proposed amendments in 2004 that covered data privacy. The Information Technology Act, 2000 (IT Act of 2000), does not specifically provide for protection of sensitive personal information”. Vivek Kumar and Dr. V.K. Gaur, “*Data Privacy in Offshore Outsourcing to India*” 32 (Corporate Law Cases, Vol.2) (2010) CLC465 (SC).

legal challenges of internet is the Information Technology (Amended) Act, 2008.<sup>359</sup>The parent I.T. Act has been conceptualized on the UNCITRAL<sup>360</sup> Model Law. This I.T. (Amended) Act, 2008 was made effective from 27 October 2009. Markable changes have been brought by the IT (Amendment) Act, 2008 to the former IT Act of 2000 on several counts<sup>361</sup>. The Information Technology Act, 2000 the only possible Act in India to address the offence relating to destruction of data as an offence, did not have any specific provisions dealing with the Data Protection. Thus in 2006, the Government introduced a bill on “Personal Data Protection Act”.<sup>362</sup> As a result two key sections were introduced in the Information Technology (Amendment) Act, 2008. Viz; Section 43A<sup>363</sup> and 72A<sup>364</sup>.

---

<sup>359</sup> The Information Technology (Amendment) Act, 2008, *available at* <https://internetdemocracy.in/laws/the-information-technology-amendment-act-2008/> (Last visited on March 18, 2019).

<sup>360</sup>The United Nation Commission on International Trade Law.

<sup>361</sup> S. Praveen Raj *et al.* “Comparison between Information Technology Act, 2000 & 2008” 1742.

<sup>362</sup>Information Technology Amendment Act, 2008- An act to amend the IT Act 2000, (November 8, 2009, 3:58:00 AM) (by lfxvideoblog), *available at* <https://blog.aujas.com/2009/11/08/it-amendment-act-2008-an-act-to-amend-the-it-act-2000/> (Last visited on 23/03/2019).

<sup>363</sup>Section 43-A.Compensation for failure to protect data. - Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation, not exceeding five crore rupees, to the person so affected. (Change vide ITAA 2008) Explanation: For the purposes of this section,-

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

<sup>364</sup>Section 72- A. Punishment for Disclosure of information in breach of lawful contract.-Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person shall be punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both.

### **3.2. vi. Privacy under the Consumer Protection Act, 1986**

Consumer privacy protection is very much needed to be protected. For the very reason that while engaging themselves on an online platform in the virtual shop stores like myntra, amazon, Alibaba, and many other attractive privacy stealing monsters, the only thing they are concerned is with questions like -what they purchase, how they purchase and how they use their purchase?<sup>365</sup>

The Consumer Protection Act, 1986 is conceived as a magna carta in the arena of consumer protection<sup>366</sup> in India. Consumer protection has also been an important agenda of many international organizations, and deals with protection of privacy and building the consumer confidence<sup>367</sup>.

### **3.2. vii. Privacy under Indian Penal Code, 1860 and Indian Evidence Act, 1872**

Privacy issues were not only considered in the Indian Constitution but also the Indian Penal Code and the Evidence Act. The Information Technology Act only came in the year 2000, supra Chapter 1. Before its commencement, The Indian Penal Code of 1860 was dealing with cyber- related issues. However certain provisions of the I.P.C. and Evidence Act were changed by this I.T. Act. Section 29-A<sup>368</sup> of the Indian Penal Code, 1860 was inserted by the I.T. Act (21 of 2000) to fill up the gaps.

---

<sup>365</sup>Consumer Privacy-How to Enforce an Effective Protective Regime? , *available at* <https://cis-india.org/internet-governance/bloFor checking the unfair trade practices and 'defect in goods' g/privacy/consumer-privacy> (Last visited on August 10, 2018).

<sup>366</sup> This Act was established to check unfair trade practices in India and to spread consumer forums to empower consumers, G.K. Kapoor, "Defective Goods and Deficiency of Services Vis a Vis Consumer", *available at* [http://www.consumereducation.in/monograms/7\\_diffective\\_goods\\_and\\_deficiency\\_o\\_services\\_vis\\_A\\_Vis\\_consumer.pdf](http://www.consumereducation.in/monograms/7_diffective_goods_and_deficiency_o_services_vis_A_Vis_consumer.pdf) (Last visited on March 23, 2019).

<sup>367</sup>Karnika Seth, *Computers, Internet and New Technology and New Technology Laws* 292(Foreword by Justice Altamas Kabir) (LexisNexis).

<sup>368</sup> "Electronic record"

### **3.2.viii. Online Privacy under Securities Exchange Board of India Guidelines**

With the unstoppable growth of cyber-attacks, SEBI came up with a risk framework guideline.<sup>369</sup> Like the Information Technology Act, it too appealed for making changes and adaptation within a stipulated time.<sup>370</sup> This Act was implemented to strengthen the framework for cyber security and also to provide efficient trade in security market.<sup>371</sup>

### **3.2.ix. Privacy under R.B.I. Guidelines**

Soon after the landmark judgment on privacy as a fundamental right by the Apex Court of our Country<sup>372</sup>, R.B.I. have published its report<sup>373</sup> and panel came up with the suggestion of adopting right-based privacy framework distinctive of the more common consent-based privacy framework.<sup>374</sup> The R.B.I. in its guidelines have stated that progression in the technology have changed the manner in which data are now processed. It further highlighted that such advancement have affected in the protection of privacy as well. In its report it pointed out the concern for protection of data privacy too. The report even mentioned privacy framework and acknowledged its concern for Data controllers. The report made it clear that they shall be made responsible for maintaining transparency and shall be made responsible for breach of

---

<sup>369</sup> The guidelines were framed on 6<sup>th</sup> July 2015.

<sup>370</sup> Geetha Nondikotkur “SEBI Issues Risk Framework Guidelines” (July 8 2015), *available at* <https://www.bankinfosecurity.com/sebi-issues-risk-framework-guidelines-a-8383> (Last visited on August 10, 2018).

<sup>371</sup> SEBI issues Risk Framework Guidelines, *available at* <https://www.bankinfosecurity.com/sebi-issues-risk-framework-guidelines-a-8383> (Last visited on March 23, 2019).

<sup>372</sup> RBI Panel seeks rights- based data privacy protection in household finance, *available at* <https://www.thehindubusinessline.com/money-and-banking/rbi-panel-seeks-rightsbased-data-privacy-in-household-finance/article9831337.ece> (Last visited on August 8, 2018).

<sup>373</sup> *Id.*

<sup>374</sup> Privacy, *available at* [https://www.indiaonline.com/article/news-top-story/rbi-panel-seeks-rights-based-privacy-framework-for-household-finance-117082600168\\_1.html](https://www.indiaonline.com/article/news-top-story/rbi-panel-seeks-rights-based-privacy-framework-for-household-finance-117082600168_1.html) (Last visited on May 16, 2019).

security during processing of the data. The R.B.I. in its report also highlighted the issues of lack of privacy laws in India and stated:

*“Continued lack of clear privacy regulations presents an ever-increasing risk to personal privacy and in most countries, privacy and data protection regulations restrict the extent to which data are available for both transactional and research purposes”.*<sup>375</sup>

### **3.3. Legal Framework for Data Protection: Indian Scenario**

There is not a single statute in India to cover the issues of Data and Data privacy in India. However, Information Technology Act, 2000 have made an attempt to define the term “data” under section 2 (o) of the Act.

#### **3.3.i. Data privacy under Information Technology Act, 2000 (Act No. 21 of 2000)**

In India there is no data protection laws but have the Information Technology Act 2000 to legalize e-Commerce. Privacy and data privacy are the two important terms in this internet age but have not defined so far under this act nor are the related issues addressed. Privacy and data privacy under this Act is only limited to section 66 (E)<sup>376</sup>, which deals with punishment in violation of privacy, e.g., voyeurism. Intermediaries are also liable in certain circumstances under this Act but are not absolute. Another issues in this Act is, it does not include BPO industries who are engaged in dealing

---

<sup>375</sup>Supra Note at 367.

<sup>376</sup>Section 66E. Punishment for violation of privacy.—Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both; Explanation.—if any individual(s) are found guilty and responsible for *transmitting or capturing or both, any private part of individual* with the help of internet in *electronic form* shall be deemed to have violated privacy of a person(s)

with huge data of data subjects. These kinds of activities have generated issues of data theft but are not addressed by this Act.<sup>377</sup> However, efforts were made by the National Association of Software and Service Companies (NASSCOM) in June 2000, where they have insisted to the government on passing of data protection law for ensuring privacy of information that travels through computer networks and thereby to meet European data protection law. I.T. Action Plan was also initiated in the year 1998. Till date there is no legislative measures which have been initiated on privacy and data matter.<sup>378</sup>

While discussing the issue of privacy, Section 66 C<sup>379</sup> and 66 D<sup>380</sup> of the Information Technology Act, 2000 is also important because of the reason that this section addresses the issues of data theft and cheating by personation. Both of these issues are connected with the privacy and data issues and are a crime punishable under this Act.

### **3.3.ii. Data privacy under Information Technology (Amended) Act, 2008**

As stated earlier, the Information Technology Act, 2000 (Act No. 21 of 2000) was enacted in the year 2000 and subsequently amended on many occasions. The most remarkable amendments were brought in the year 2008, and the Act came to be known as the Information Technology Amended Act, 2008. The original Act was amended for the simple reason that it could not regulate e-Commerce and cyber crimes as it had thought.

---

<sup>377</sup>Barkha and U. Rama Mohan, "Cyber Law & Crimes" 164 (Published by S.P. GOGIA (H.U.F.) (Reprinted on, 2012 & 2013).

<sup>378</sup>*Id.* at 165

<sup>379</sup> "Punishment for identity theft"

<sup>380</sup> "Punishment for cheating by personation by using computer resource" .-Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.



India does not have any uniform law on privacy and data protection unlike the European Union but has different statute like that of the United States which covers the issues of privacy and data in pieces.<sup>381</sup> Section 2 (o) of the Act defines the term data as knowledge or information but nowhere it neither talks about the privacy nor defines it. Data Privacy under the Information Technology Act, 2008 is not addressed at all. Both data and privacy are not considered to be part and parcel. What the original Act has done is defined the term “data” under section 2 (0) and by its amendment inserted section 66 E, which prescribes the punishment for the violation of confidentiality and privacy. In a nutshell it is concluded that the Information Technology Act, 2008 lacks provisions for data privacy and in this technologically driven society it is mandatory to have a law which can compete with the threats posed by the internet.

### **3.3.iii. White Paper on Data Protection (November 27, 2017)**

The issue of data protection in India was re-addressed in the year 2017 wherein a white paper on data protection was initiated by the Government. This paper was a petition appealing the public to put forward their valuable opinion on data protection law. To carry out the agenda of this paper Justice Shri B.N. Srikrishna<sup>382</sup> led a committee.<sup>383</sup> The issue of informational privacy was addressed by the Supreme Court in *Puttaswamy* case supra.

---

<sup>381</sup> Benjamin Wilson, *Data Privacy in India: The Information Technology Act*, (Posted on February 8, 2019), available at [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3323479](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3323479) (Last visited on January 27, 2020).

<sup>382</sup>*Id.*

<sup>383</sup> The Government of India constituted a committee mainly for addressing data related issues like lack of its protection regime and the urgent need of having a data protection law. In this regard, the committee suggested a draft on Data Protection Bill. The main aim of the committee was twofold. The first was to ensure digital economy and the second was to protect data of personal nature, White Paper on Data Protection Framework for India-Public Comments Invited, available at

The draft on Personal Data Protection Bill, 2018 has been submitted to the Ministry of Electronics and Information Technology (MEITY), which is claimed to be a fourth way report not based on European Union model, United States model or the Chinese model. This proposed framework is purely considered to suit the Indian demands and of other developing countries.<sup>384</sup>

The report of this committee is very extensive in its approach and envelops every corner of the Privacy issues and Data protection. Grounds of Processing, types of Data Protection, Regulation and Enforcement and Legal Remedies available to citizens of the nation are addressed by this report. Growth of digital economy through experimentation and innovation and security of citizens data are the main objectives of this committee. The importance of data protection in the age of Digital Revolution is the laid impetus of this report. At first the committee dived into the history of Privacy and Data Protection and came out to know that it was in the 1970's that there was an increased use and collection of data containing personal information.<sup>385</sup>. The report laid a lot of importance on the flexibility of legal instruments to be in consonance with the changing time and technological advancement. The Report is an analysis of the existing privacy laws in European Union and the United States. In the initial phase this report tried to define data and types of data available, processing of data and how it is to be done. Major two areas covered in this report were data and privacy only. Apart from this, the Report also defines Personal Data and its types, sensitive data and cross-border transfer of personal information. The Committee observed that regulations of the European Union have recognized other rights such as

---

<https://meity.gov.in/white-paper-data-protection-framework-india-public-comments-invited> (Last visited on 14/03/2019).

<sup>384</sup>The Information Technology (Amendment) Act, 2008.

<sup>385</sup> Robert Gellman, "Fair Information Practices: A basic History", *available at* <https://bobgellman.com/rg-docs/rg-FIPshistory.pdf> (Last visited on March 18, 2019).

the right to object to data processing. Incorporation of such rights in Indian law requires further assessment. It also noted that the right to be forgotten has emerged as a contentious issue in data protection laws. The committee further discussed the penalties for offences under the proposed law, and the authority which should have the power to hear and adjudicate complaints.

### **3. 4. Privacy and Data Protection - International Scenario**

Many International Organization, Documents and instruments like WTO, OECD, WIPO, and APEC etc. have played an active role in propounding the fundamental principles for States to frame or enact their legislations to govern internet activity. These organizations in a way makes vows that e-Commerce shall progress in cyberspace even in cases of hurdles.<sup>386</sup>

The advancement in the pace of technology has brought up a wide array of privacy issues. The insidious practice includes unimaginable breaches such as misuse of an individual's genetic information<sup>387</sup>, or damage of digital persons etc. and in view of the fact that human life is related to Laws, it raises some questions towards law and that too in every form of law. These issues are diverse and concern not only the legal issues but involves ethical and social too. Among these issues, the legal one stands out on different pedestal as law can only strike a balance between scientific advancement on the one hand, and its possible misuse on the other. Various laws such as criminal law and human rights and other related laws need to be thoroughly revised in order to answer all the legal issues concerning the importance of protection

---

<sup>386</sup>Karnika Seth, *Computers, Internet and New Technology Laws* 20 (Foreword by Justice Altamas Kabir) (LexisNexis).

<sup>387</sup> E.J. Jathin, "Human Genome Project: Emerging Challenges of Right to Privacy vis-à-vis Insurer's Right to Know" 1-3, *Cochin University Law Review*, (March-June) (2007) (Number 1 & 2) (Vol. XXXI), (Eds. D. Rajeev, N.S. Gopalakrishnan et. all) (2007).

of an individual's right to privacy in this genetic era<sup>388</sup> and its related commercial issues. Apart from the commercial issues, there are issues relating to right to privacy. Unlike U.K., New Zealand and Australia, India does not have a particular legislation to deal with the issues of genetic discrimination or misuse of genetic information. The existing Constitutional provisions protect privacy and equality in general. As such International Documents have to be referred to in addressing the issues of Privacy protection and Data protection concerning protection of Human Rights in India.

Altogether nine international documents and international organizations have been discussed below. They are;-

#### **3.4.i. World Trade Organization, (W.T.O.)**

WTO provides an extensive knowledge of global trade<sup>389</sup>. Supranational body in the form of W.T.O. was created to enforce international cooperation in electronic commerce.<sup>390</sup> Business which takes place online includes jurisdiction issue among other legal one. W.T.O. has been regulating goods market for decades and still is working in the era of e-Commerce.<sup>391</sup> There are agreements<sup>392</sup> entered into by W.T.O. Apart from the Statutes International Organizations like W.T.O. are continuously

---

<sup>388</sup> *Supra* Note at 377.

<sup>389</sup> Rolf H. Weber & Romana Weber, *Internet of Things* 30 (Published by Springer-Verlag Berlin Heidelberg) (2010).

<sup>390</sup> Yun Zhao, "Dispute Resolution in Electronic Commerce" (Volume 9) (Martinus Nijhoff Publishers LEIDEN/ t).

<sup>391</sup> WTO Appellate Body Repertory of Reports and Awards 1995-2010, available at [https://books.google.co.in/books?id=xMNOdF7vuXkC&pg=PA267&lpg=PA267&dq=%E2%80%9Ca+responding+party+must+make+a+prima+facie+case+that+its+challenged+measure+is+%E2%80%98necessary.%E2%80%99%E2%80%9D&source=bl&ots=9CJw\\_QFWIE&sig=IgwNd88G-xIx8bBAp5PDs9JV67c&hl=en&sa=X&ved=0ahUKEwiQoaGG9szXAhURTo8KHT\\_fAzwQ6AEIJzAA#v=onepage&q=%E2%80%9Ca%20responding%20party%20must%20make%20a%20prima%20facie%20case%20that%20its%20challenged%20measure%20is%20%E2%80%98necessary.%E2%80%99%E2%80%9D&f=false](https://books.google.co.in/books?id=xMNOdF7vuXkC&pg=PA267&lpg=PA267&dq=%E2%80%9Ca+responding+party+must+make+a+prima+facie+case+that+its+challenged+measure+is+%E2%80%98necessary.%E2%80%99%E2%80%9D&source=bl&ots=9CJw_QFWIE&sig=IgwNd88G-xIx8bBAp5PDs9JV67c&hl=en&sa=X&ved=0ahUKEwiQoaGG9szXAhURTo8KHT_fAzwQ6AEIJzAA#v=onepage&q=%E2%80%9Ca%20responding%20party%20must%20make%20a%20prima%20facie%20case%20that%20its%20challenged%20measure%20is%20%E2%80%98necessary.%E2%80%99%E2%80%9D&f=false) (Last visited on November 20, 2017).

<sup>392</sup> "GATT", "TRIPS"

working towards protection of one's personal information and data which deserve privacy and protection.

E-Commerce is another stem sprouting from W.T.O.<sup>393</sup> Many countries are a signatory to W.T.O. All these countries have agreed to adhere and inculcate its norms in conducting of the business. "*Tariff*" and "*National Treatment*", are the two most prominent characters of W.T.O.<sup>394</sup>

The inevitable question that arises in e-Commerce is that of products being delivered electronically through the internet stage. The argue is basically on the inefficiency of GATT<sup>395</sup> on providing adequate framework for dealing with the market access vis-à-vis electronic commerce.

The issue with W.T.O. is that its mechanism for e-Commerce is exclusively available to member states. Therefore private dispute needsto be supported by its member states. With regard to the dispute resolution under W.T.O. "Yun Zhao" in his book titled "Dispute Resolution in Electronic Commerce", appreciate the "*new mechanism for resolving disputes*" and find it as an umbrella for all the multilateral and plurilateral agreements.<sup>396</sup>

---

<sup>393</sup> Alwyn Didar Singh *E-Commerce In India: Assessment and Strategies for the Developing World* 778-782 (2008) (LexisNexis, Butterworths Publication).

<sup>394</sup> 'National Treatment' in the context of giving equal treatment to international based service providers compared to domestic.

<sup>395</sup> "General Agreement on Tariffs and Trade"

<sup>396</sup> Yun Zhao, "Dispute Resolution in Electronic Commerce" 63 (Volume 9) (Martinus Nihhoff Publishers, LEIDEN/ BOSTON) (Printed and bound in the Netherlands).

### 3.4.ii. Organization for Economic Cooperation and Development (OECD)<sup>397</sup>

*“The OECD is an organization focused predominantly on economic matters. The members countries are quite diverse and combined they produce approximately two-thirds of world goods and services. Consequently, concerns about the potential effects of the rise of the private enterprise were central to the OECD’s interest in privacy”.*<sup>398</sup> Privacy guidelines 1980, has been one of the highlighted features of OECD<sup>399</sup>. Its guidelines were drafted in 1979<sup>400</sup>. OECD<sup>401</sup> came as torchlight to highlight the importance of data privacy. Established in 1961, it has now 30 leading nations as its members<sup>402</sup>. It produced a set of guidelines which became a touchstone of privacy discourse since then.

In the context of e-Commerce, OECD focuses on the need for global cooperation to enable consumer to truly exercise his/her rights in the electronic market place. In an online transaction privacy of one has to be protected. Service provider seeks personally identifying information about the user on the condition that it shall be kept private and will not be used for any other purposes other than agreed upon by the users. OECD ensures that such privacy policy of a service provider on web page

---

<sup>397</sup>In 1978, the Organization for Economic Cooperation and Development (OECD) convened a group of experts to study developments in different countries and to produce guidelines that might form a consensus position on privacy issues, with a view to facilitating harmonization of national laws in this area. In 1980, the OECD published its *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. The Guidelines are the basic source of the fair-information principles at the heart of debates about commercial use of personal information.

Ronald J. Mann, “Electronic Commerce” 303(Third Edition) (2008) (Aspen Publishers) (Printed in the United States of America).

<sup>398</sup>Karnika Seth, *Computers, Internet and New Technology Laws* 292 (Foreword by Justice Altamas Kabir) (LexisNexis).

<sup>399</sup>*Id.*

<sup>400</sup> Prof. Vimlendu Tayal, *Cyber Law, Cyber Crime, Internet and E-Commerce* 34 (Published by Bharat Law) (First Published 2011).

<sup>401</sup>Yee Fen Lim “Cyberspace Law” Commentaries and Materials, 143 (Second Edition) (First Edition 2008) (Originally Published by Oxford University Press, Australia 2007) (Printed in India by Vishal Binding House, Noida).

<sup>402</sup>Raman Mittal & Neelotpal Deka, *Cyber Privacy, Legal Dimensions of Cyberspace* 205 (S.K. Verma& Raman Mittal (eds.) (Indian Law Institute, India).

assures privacy policy and that there are remedies available in the event of a breach of confidence. OECD also considers trans-border data flow contracts and ensures that contracts determining the principle on privacy and personal information are passed trans-border data flows. OECD also stresses on the need to educate users of the risks in trans-border data flows. OECD<sup>403</sup> also stresses on the need to educate users of the risks in trans-border data flows. OECD also stresses on the need to educate users of the risks in from one data controller to another only on the occasion of fulfillment of legal requirements for trans-border data flows. OECD<sup>404</sup> also stresses on the need to educate users of the risks in dealing on the internet, their rights to privacy and the technological and legal means to protect those rights.<sup>405</sup>

Articles 19 (1) (a) and 21 supra chapter 2, are the two most crucial articles of Indian Constitution. It took several years for the legislation and judiciary to read “privacy” in the context of these articles. International bodies have also given recognition to these rights Under Articles, 12<sup>406</sup>, 17<sup>407</sup>, 8<sup>408</sup>, 111<sup>409</sup> and, 10<sup>410</sup>.

Privacy<sup>411</sup> is not an easy term to define, its definition vary from person to person depending on the society an individual is subjected to.<sup>412</sup>

---

<sup>403</sup> T. Ramappa, *Legal Issues in Electronic Commerce* 86 (First Published 2003) (Published by Rajiv Beri for Macmillan India Ltd.).

<sup>404</sup> *Id.*

<sup>405</sup> *Id.* at 85.

<sup>406</sup> “Universal declaration of Human Rights 1948”

<sup>407</sup> “International Convention on Civil and Political Rights-1966”

<sup>408</sup> “European Convention of Human Rights-1950”

<sup>409</sup> “American Convention on Human Rights-1969 African Charter on Human Rights”

<sup>410</sup> “Welfare of Child-1990”

<sup>411</sup> Right of Privacy and Internet available at [https://shodhganga.inflibnet.ac.in/bitstream/10603/58938/11/11\\_chapter%206.pdf](https://shodhganga.inflibnet.ac.in/bitstream/10603/58938/11/11_chapter%206.pdf) (Last visited on April 29, 2007).

<sup>412</sup> *Id.*

The relief is in the fact that every Country is making an effort for its protection and recognition and the issue is with the increasing intrusion into one's privacy, data theft, breach of confidentiality and much more.

OECD<sup>413</sup> guides the two bodies of the Government viz; Legislature and the Judiciary to make law and to interpret depending on the need and necessity.<sup>414</sup> Among its principles most important one is “*Disclosure and transparency*”<sup>415</sup>.

The importance to ‘personal data privacy’ was spotted a decade ago by the Organization for Economic Cooperation and Development (OECD) by way of producing a set of guidelines<sup>416</sup>. It is not a surprising thing to have different laws for different countries. The problem arises when economic transaction takes place among countries having different governing laws. The year 1970 marked the terror among national laws for having disparities on personal laws, and feared the restriction for hindrance on cross-border flow of information, which might disrupt important factors of the economy. To this issue OCED came as a relief not in the form of Convention but with a feather of guidelines.<sup>417</sup>

---

<sup>413</sup> It aims at, Basic rights, Right to be informed and Right to Participate, *available at* <https://www.youtube.com/watch?v=T8rMS2nKMmI> (Last visited on October 6, 2018).

<sup>414</sup> OECD Principles, Knowledge Equity (Published Mar. 16, 2016), *available at* <https://www.youtube.com/watch?v=T8rMS2nKMmI> (Last visited on October 6, 2018).

<sup>415</sup> *Id.*

<sup>416</sup> These guidelines have remained the touchstone of privacy discourse since then. The OECD is an organisation focused predominantly on economic matters. The members countries are quite diverse and combined they produce approximately two-thirds of world goods and services. Consequently, concerns about the potential effects of the rise of the private enterprise were central to the OECD's interest in privacy.

The OECD Privacy Framework, *available at* [https://www.oecd.org/sti/ieconomy/oecd\\_privacy\\_framework.pdf](https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf) (Last visited on February 11, 2019).

<sup>417</sup> OECD merely recommends but that countries take its basic principles into account. They are not obligatory; countries need not apply all or any of the rules. The nature of an aspirational document is such that it often lacks detail and uses broad, flexible language. This is not necessarily a criticism of the OECD guidelines; rather, this feature has enabled it to stand the test of time, and it remains one of the seminal documents in the privacy discourse. The OECD Privacy Framework, *available at* [https://www.oecd.org/sti/ieconomy/oecd\\_privacy\\_framework.pdf](https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf) (Last visited on February 11, 2019).



OECD in its guidelines for the Consumer's/e-User's, especially in "*Electronic Commerce*" focused mainly on the necessity for having a global cooperation to facilitate the consumer to truly exercise their rights in the electronic market place. To achieve these objectives it further focused on modifying their existing legal framework and on fostering self-regulatory practices, whereby members countries were invited through their judicial, regulatory and law enforcement authorities to cooperate at the international level as appropriate through information exchange, coordination, communication and joint action to combat cross-border fraudulent, misleading and unfair commercial conduct and also to make use of existing international networks and enter into bilateral and/multilateral agreements or other such arrangements as necessary and appropriate, to accomplish such cooperation.<sup>418</sup>

Government alone cannot boost up the confidence of buyer in dealing on Internet. Voluntary of unguided electronic purchasing, their rights and the redressing bodies for relief on failure of handicapped and its movement too has not taken roots due to number of reasons like, different languages, lack of resources, financial and manpower.<sup>419</sup>

On the internet, privacy of users has to be protected. Service providers ask the user certain questions captioned as "personally identifying information", based on the relevant need and subject to the condition of its being kept private and not being used further for purposes other than the matter for which it was collected. Information such as those including spending habits, income, and medical history, special treatments are of private nature and in no way can be used for any purpose not intended and

---

<sup>418</sup> T. Ramappa, *Legal Issues in Electronic Commerce* 86, (First published, 2003), (Published by, Rajiv Beri for Macmillan India Ltd. 2/10).

<sup>419</sup> *Supra* Note at 416.

communicated to the user.<sup>420</sup> For safety purpose the users are needed to check the privacy policy of a service provider on his web page and adhere carefully on the available assuring privacy policy, and remedies available on event of breach of confidence.

On *Protection of Privacy on Global Networks* 1998, OECD stated that ‘privacy could be enhanced by technological means as well as contractual provisions’.<sup>421</sup> To add on this there are two more way of enhancing privacy technologies, i.e. either self-regulatory or legislative approaches which will enable users to protect their privacy and personal data, for instance providing mechanisms for user secrecy, encryption, or automated application of user privacy preferences. When it comes to commercial contracts, OECD considers that model trans-border data flow contracts which determines the principles to be applied on event of personal information being passed from one data controller to another plays a significant role in protection of privacy and in satisfying legal requirements for trans-border data flows. OECD also address the need to educate users of the risks involved in dealing on the internet, their rights to privacy and the technological and legal means to protect those rights.<sup>422</sup>

At present a broad range of products are available online and only one click away from the potential users/buyers, but still due to lack of privacy protection mechanism in the electronic marketplace e-users have not fully embraced the idea of buying online. Further this fear is coupled with questions like, the accuracy of information , contract formation, the availability of redress and dispute resolution mechanisms, the

---

<sup>420</sup>*Supra* Note at 140.

<sup>421</sup>*Id.*

<sup>422</sup>*Supra* Note at 419.

potential for fraud and privacy issues.<sup>423</sup> As such consumers are alarmed about the practicalities and safety of the electronic environment and reluctant in full involvement in the electronic commerce. The reality today is, in electronic commerce risks is greater than its value and that the consumer buying online are faced with problems which cannot be solved by him all alone. The contrasting nature of legal obligations of buyers and sellers in different jurisdiction further raise complex issues of applicable law and jurisdiction, and effective means of enforcement of the rights etc. And these issues can be addressed, only through international agreements and common set of rules of trade in electronic market place and will reduce uncertainty, conflict and litigation for necessary consistency in legal rules.<sup>424</sup>

The problem with OECD is that its guidelines are often not easy to apply to contemporary data-collection practices because statutes based on the Guidelines typically focus on regulation of the activities of any “data controller” and this concept is difficult to apply to modern organizations that collect information from a variety of sources in open network environments. The volume of information collected online about individuals and their distribution and storage create huge security problem. The right to access and correct data about individuals is another issue in this contemporary digital world.<sup>425</sup>

---

<sup>423</sup>*Id.*

<sup>424</sup> Supra Note at 140.

<sup>425</sup>The problem of protecting individual’s data is not a big issue in the United States as it is in India. Where as in Europe they have OECD Guidelines which is a guiding torch to protect their data. Ronald J. Mann *Electronic Commerce* 303 (Aspen Publishers, New York) (2008).

The OECD consists of a council, Committee and a Secretariat. One of its strength includes its peer review progress, through which the performance of countries is monitored by other countries at the commercial-level<sup>426</sup>.

### **3.4.iii. Asia-Pacific Economic Cooperation (APEC)**<sup>427</sup>

APEC has also framed its privacy policy of 1994, just like OECD's policy on privacy of 1980<sup>428</sup>. All together there are 21 member Countries. To name few are USA and Australia.<sup>429</sup> It was formed to address and discuss the issues relating to trade for its liberation. It facilitates free trade across Asia-Pacific region<sup>430</sup>. India was not included as its member. It was not a trading economy, and it can be understood from its omission in the APEC, 1989.<sup>431</sup> Sandeep Gopalan (VC Deakin University, Melbourne Australia) stated that in order to eradicate "*poverty*", India has to be a member of "*APEC*".<sup>432</sup>

---

<sup>426</sup>Rolf H. Weber & Romana Weber, *Internet of Things* 31-32 (Published by Springer-Verlag Berlin Heidelberg) (2010).

<sup>427</sup> In 1989, it was established for few reasons, i.e. for providing opportunity to its member countries, for attaining sustainable development, *available at* <https://www.apec2018png.org/apec-2018> (Last visited on March 23, 2019).

<sup>428</sup>Karnika Seth, *Computers, Internet and New Technology Laws* 292 (Foreword by Justice Altamas Kabir) (LexisNexis).

<sup>429</sup>In 1998 the admission of Russia, Vietnam and Peru expanded this club, *available at* <https://www.tribuneindia.com/news/comment/time-to-bust-myth-that-india-doesn-t-belong-in-apec/689954.html> (Last visited on March 23, 2019).

<sup>430</sup> Asia-Pacific Economic Cooperation, *available at* [https://en.wikipedia.org/wiki/Asia-Pacific\\_Economic\\_Cooperation](https://en.wikipedia.org/wiki/Asia-Pacific_Economic_Cooperation) (Last visited on March 23, 2019).

<sup>431</sup>*Available at* <https://www.tribuneindia.com/news/comment/time-to-bust-myth-that-india-doesn-t-belong-in-apec/689954.html> (Last visited on March 23, 2019).

<sup>432</sup>Time to bust myth that India does not belong in APEC, *available at*, <https://www.tribuneindia.com/news/archive/time-to-bust-myth-that-india-doesn-t-belong-in-apec-689954> (Last Visited on February 14, 2020).

### 3.4.iv. World Intellectual Property Organization (WIPO)<sup>433</sup>

WIPO was established to protect intellectual creations such as artistic and literary works. The organization also promotes the international agreements on copyright, patents and trademarks, etc. It has more than 110 countries as its member and provides technological information and assistance to developing countries<sup>434</sup>.

Countries have laws to protect their intellectual property. WIPO deals with the issue of intellectual property.<sup>435</sup> It is protected for two motives; one is for obtaining legal sanction and another for protection of the invention. It is a deliberate act of Government which encourages fair trading and contributes to economic and social development.<sup>436</sup>

Intellectual Property<sup>437</sup> (hereinafter captioned as 'IP') are those property which are human creation.<sup>438</sup> IP and e-Commerce are interrelated<sup>439</sup> and is very important to one another for several reasons. IP is also involved in making e-Commerce work.<sup>440</sup>

---

<sup>433</sup> Available at <https://www.drishtiiias.com/important-institutions/drishti-specials-important-institutions-international-institution/important-institutions-international-world-intellectual-property-organisation-wipo> (Last visited on May 23, 2019).

<sup>434</sup> Suresh T. Viswanathan, *The Indian Cyber Laws* 137 (Foreword by N. Chandrababu Naidu) (First Edition 2000) (Published by D.C. Puliani for Bharat Law House) [The Intellectual Property aspects in Cyber Law (The WIPO Initiative)].

<sup>435</sup> Yun Zhao, "Dispute Resolution in Electronic Commerce" 65 (Volume 9) (MARTINUS NIJHOFF PUBLISHERS, LEIDEN/ BOSTON).

<sup>436</sup> WIPO, Intellectual Property Handbook, available at [https://www.wipo.int/edocs/pubdocs/en/intproperty/489/wipo\\_pub\\_489.pdf](https://www.wipo.int/edocs/pubdocs/en/intproperty/489/wipo_pub_489.pdf) (2004, 2<sup>ND</sup> Edition) (Reprinted 2008), (Last visited on March 26, 2019).

<sup>437</sup> WIPO Intellectual Property Handbook, available at [https://www.wipo.int/export/sites/www/sme/en/e\\_commerce/pdf/ip\\_ecommerce.pdf](https://www.wipo.int/export/sites/www/sme/en/e_commerce/pdf/ip_ecommerce.pdf) (2004, 2<sup>ND</sup> Edition) (Reprinted 2008) (Last visited on March 26, 2019).

<sup>438</sup> It includes patents, patents, trademarks, industrial designs, and geographical indications. WIPO Intellectual Property Handbook, (2004, 2<sup>ND</sup> Edition) (Reprinted 2008), available at [https://www.wipo.int/export/sites/www/sme/en/e\\_commerce/pdf/ip\\_ecommerce.pdf](https://www.wipo.int/export/sites/www/sme/en/e_commerce/pdf/ip_ecommerce.pdf) (Last visited on March 26, 2019).

<sup>439</sup> IP Concerns about International Transaction in E-Commerce, available at [https://www.wipo.int/sme/en/e\\_commerce/transactions.htm](https://www.wipo.int/sme/en/e_commerce/transactions.htm) (Last visited on March 26, 2019).

<sup>440</sup> WIPO Intellectual Property Handbook, (2004, 2<sup>ND</sup> Edition) (Reprinted 2008), available at [https://www.wipo.int/export/sites/www/sme/en/e\\_commerce/pdf/ip\\_ecommerce.pdf](https://www.wipo.int/export/sites/www/sme/en/e_commerce/pdf/ip_ecommerce.pdf) (Last visited on March 26, 2019).

E-Commerce occurs globally and this characteristic makes it one of the most remarkable one in the internet world. Likewise IP is used and licensed in many countries. The global character of e- of protection and dispute relating to e-Commerce and IP is affected by the issue of court's jurisdiction and the laws which affect IP vary from country to country<sup>441</sup>.

WIPO is closely related with e-Commerce for the reason that many disputes arising out of e-Commerce relates to the protection of intellectual property. International commercial disputes between private parties were resolved even back in 1994, with the WIPO centre for arbitration and mediation based in Geneva, Switzerland. This centre was mainly focused on the administration of disputes relating to the internet and e-Commerce.

Intellectual Properties are protected under the umbrella of its comprehensive guidelines on "piracy".<sup>442</sup> Lots of other initiatives have also been under taken by WIPO<sup>443</sup>, in this regard for the protection of the "intellectual property".<sup>444</sup>

#### **3.4.v. Trade Related Intellectual Property Rights (TRIPS)**

TRIPS include legal agreement between W.T.O. member nations and such agreements are of international nature. As such it requires the governments of the member nations to inculcate minimum standards like those applied to *nationalsof*

---

<sup>441</sup>IP Concerns about International Transaction in E-Commerce, *available at* [https://www.wipo.int/sme/en/e\\_commerce/transactions.htm](https://www.wipo.int/sme/en/e_commerce/transactions.htm) (Last visited on March 26, 2019).

<sup>442</sup> Dr. S.V. Joga Rao, "Law of Cyber Crimes & Information Technology Law" 234-235.

<sup>443</sup> "WIPO copyright Treaty (WCT)" and the "WIPO Performances and Phonograms Treaty (WPPT)"

<sup>444</sup> Dr. S.V. Joga Rao, "Law of Cyber Crimes & Information Technology Law" .234-235.

other WTO member nations.<sup>445</sup> General Agreement on Tariffs and Trade (GATT) during the year 1989 and 1990 has played a very important role in shaping the TRIPS at Uruguay Round. For the first time in history Intellectual Property (IP) was initiated by the TRIPS agreement in a multi trading system. Doha Declaration is another important result of the initiative taken by the developing countries on the TRIPS agreement. The declaration laid down the scope of the TRIPS and highlighted its goal. One of the goals was to promote technological innovation and IPR's. The most important goal which seems practical in this technological era has been the protection of confidential information.<sup>446</sup> Dispute settlement mechanism is another important aspect that has been covered by<sup>447</sup> the TRIPS Agreement.<sup>448</sup>

#### **3.4.vi. European Convention on Human Rights (ECHR)**

Article 8<sup>449</sup> of the European Convention on Human Rights (ECHR) lays down the basis for one of the most progressive privacy regimes in the world. "Privacy is not treated as an absolute right and is subject to certain restrictions that are considered necessary in a democratic society. The application of these exceptions is to be in accordance with specific laws enacted in this regard."<sup>450</sup> At the juncture of technological menace, lies the issue of Privacy. Privacy and confidentiality shares an important bonding, where confidentiality is an important tool for protecting

---

<sup>445</sup> Available at <http://www.worldtradelaw.net/uragreements/tripsagreement.pdf>.download (Last visited on June 16, 2019).

<sup>446</sup> *Id.*

<sup>447</sup> Article-8. Exhaustion .- For the purposes of dispute settlement under this Agreement, subject to the provisions of Articles 3 and 4 nothing in this Agreement shall be used to address the issue of the exhaustion of intellectual property rights.

<sup>448</sup> World Trade Organisation, (10 February 1999) (IP/C/W/128), The Work Programme on Electronic Commerce, Councils for Trade Related Aspects of Intellectual Property Rights, *available at* [https://www.wto.org/english/tratop\\_e/trips\\_e/ta\\_docs\\_e/8\\_1\\_ipcw128\\_e.pdf](https://www.wto.org/english/tratop_e/trips_e/ta_docs_e/8_1_ipcw128_e.pdf) (Last visited on March 26, 2019).

<sup>449</sup> "Right to Respect for Private and Family Life"

<sup>450</sup> Rishika Taneja and Sidhant Kumar, *Privacy Law, Principles, Injunctions and Compensation* 9, (EBC Publishing (p) Ltd., Lucknow) (Printed by, Gopsons Papers Ltd., A-2, Sector-64, Noida) (1<sup>st</sup> Edn. 2014).

privacy.<sup>451</sup>Article 8<sup>452</sup> of the European Convention on Human Rights specifically deals with the data processing activities of private sector bodies, whereas Article 8 (1) argues on purchaser /browser-related data in context with ECMS (Electronic Copyright Management Systems) and discusses about the interference with the data subject's right to respect for private life on fulfillment of certain conditions like:

- 1) the data reveal details about the data subject's personality (e.g. his/her preferences);
- 2) the data are processed without the data subject's knowledge or consent; and
- 3) the processing potentiality casts the data subject in a negative light or could result in a restriction of data subject's freedom of choice.<sup>453</sup>

Article 8<sup>454</sup> of the European Convention on Human Rights specifically deals with the data processing activities of private sector bodies, whereas Article 8 (1) argues on purchaser /browser-related data in context with ECMS (Electronic Copyright Management Systems) and discusses about the interference with the data subject's right to respect for private life on fulfillment of certain conditions like:

- 1) the data reveal details about the data subject's personality (e.g. his/her preferences);
- 2) the data are processed without the data subject's knowledge or consent; and
- 3) the processing potentiality casts the data subject in a negative light or could result in a restriction of data subject's freedom of choice.<sup>455</sup>

---

<sup>451</sup> Supra Note at 18.

<sup>452</sup> Supra Note at 160.

<sup>453</sup> Lee A. Bygrave and Kamiel J. Koelman, *Privacy, Data Protection and Copyright: Their Interaction in the Context of Electronic Copyright Management Systems, Copyright and Electronic Commerce, Legal Aspects of Electronic Copyright Management*, 94 (Editor, P. Bernt Hugenholtz),(2000), (Published by, Kluwer Law International Ltd., London, United Kingdom)

<sup>454</sup>Supra Note at 169.

<sup>455</sup>*Id.*.



### 3.4.vii. International Criminal Police Organization (INTERPOL)<sup>456</sup>

INTERPOL is the world largest International Police Organization<sup>457</sup>. It has been keenly engaged in combating cybercrimes. In 1981, it held its first training seminar for investigators of Computer Crime. Followed by the International conference on Computer Crimes on 1995, 1996, 1998, 2000 and 2003. It has also set up a ‘*working parties*’<sup>458</sup> or a group of experts at regional level in addressing the issues of cyber crimes.<sup>459</sup> Its member countries maintain a National Central Bureau known as NCB<sup>460</sup>. Cyber attack knows no boundaries and the issue is that of hacking and other traditional crimes which pose threats to victims worldwide<sup>461</sup>. Interpol is working actively to combat cybercrimes in America<sup>462</sup>. There are number of working parties under INTERPOL, it includes European Working Party for Information Technology Crime, American Regional Working Party on Information Technology Crime, African Regional Working Party on Information Technology Crime and Asia-South Pacific Working Party on Information Technology Crime.

---

<sup>456</sup>The International Criminal Police Organization (*Organisation internationale de police criminelle*), more commonly known as Interpol, is an international organization that facilitates police cooperation. It was established in 1923 as the International Criminal Police Commission (ICPC); it chose INTERPOL as its telegraphic address in 1946, and made it its common name in 1956. The mandate and the primary task of INTERPOL is to support police and law enforcement agencies in its 186 member countries in their efforts to prevent crime and conduct criminal investigations as efficiently and effectively as possible. Specifically, INTERPOL facilitates cross border police cooperation and, as appropriate, supports governmental and intergovernmental organizations, authorities and services whose mission is to prevent or combat crime. The International Criminal Police Organization, available at [https://www.un.org/sc/ctc/wp-content/uploads/2017/02/icpo\\_background-Information.pdf](https://www.un.org/sc/ctc/wp-content/uploads/2017/02/icpo_background-Information.pdf) (Last visited on March 26, 2019).

<sup>457</sup>*Id.*

<sup>458</sup>Available at <https://www.interpol.int/News-and-Events/News/2018/INTERPOL-project-to-combat-cybercrime-in-the-Americas> (Last visited on March 26, 2019).

<sup>459</sup>*Supra* Note at 64.

<sup>460</sup>*Id.*

<sup>461</sup>Cybercrime, available at <https://www.interpol.int/Crimes/Cybercrime> (Last visited on March 26, 2019).

<sup>462</sup>INTERPOL Projects to combat cybercrime in the Americas, (18<sup>th</sup> October 2018), available at <https://www.interpol.int/News-and-Events/News/2018/INTERPOL-project-to-combat-cybercrime-in-the-Americas> (Last visited on March 26, 2019).

### 3.4.viii. G7 &G8 Group

The chief advisors of science of G7 countries along with Russia and the European Union under the P8<sup>463</sup> established a group on Misuse of International Data Networks in 1996.<sup>464</sup> Both the groups emphasized on adopting advance technologies.<sup>465</sup> This expert group also suggested legal measures to address the international mechanism for addressing illegal actions<sup>466</sup>, strengthening international mechanisms for addressing illegal contents<sup>467</sup>, indemnifying the affected party(s) by middleman are another area of concern of these groups.<sup>468</sup> Member countries are even aided to have cyber laws,<sup>469</sup> to figure out the grey areas in terms of cyber related issues, to develop international information network<sup>470</sup>, foster cooperation<sup>471</sup>, to handle the jurisdictional issues with trained law people .

In 1997 High Tech subgroup of G8 senior experts developed ten principles on Transnational Organized Crime to combat computer crime. It aimed at ensuring that criminals will not attain a safe haven anywhere in the world. It also ensured on the legal process and technical ability of the authority in finding criminals abusing

---

<sup>463</sup> Prof. Dr. Ulrich Sieber, “Legal Aspects of Computer-Related Crime in the Information Society” – COMCRIME-STUDY- (Version 1.0 of 1<sup>st</sup> January 1998), *available at* <http://www.edc.uoc.gr/~panas/PATRA/sieber.pdf> (Last visited on March 29, 2019).

<sup>464</sup>*Id.*

<sup>465</sup> This Group on Misuse of International Data Networks consisted of legal and technical experts of the Members-States in the field of International Communication networks, *available at* <https://shodhganga.inflibnet.ac.in/bitstream/10603/188821/9/7%20chapter%205.pdf> (Last visited on January 29, 2019).

<sup>466</sup>*Available at* <https://shodhganga.inflibnet.ac.in/bitstream/10603/188821/9/7%20chapter%205.pdf> (Last visited on January 29, 2019).

<sup>467</sup>*Available at* <https://shodhganga.inflibnet.ac.in/bitstream/10603/188821/9/7%20chapter%205.pdf> (Last visited on January 29, 2019).

<sup>468</sup>*Available at* <https://shodhganga.inflibnet.ac.in/bitstream/10603/188821/9/7%20chapter%205.pdf> (Last visited on January 29, 2019).

<sup>469</sup>*Available at* <https://shodhganga.inflibnet.ac.in/bitstream/10603/188821/9/7%20chapter%205.pdf> (Last visited on January 29, 2019).

<sup>470</sup>*Available at* <https://shodhganga.inflibnet.ac.in/bitstream/10603/188821/9/7%20chapter%205.pdf> (Last visited on January 29, 2019).

<sup>471</sup>*Available at* <https://shodhganga.inflibnet.ac.in/bitstream/10603/188821/9/7%20chapter%205.pdf> (Last visited on January 29, 2019).

technologies. Other countries were also a part of this network and applied these principals of G8 to their national laws and policies through treaties.<sup>472</sup>

The May summit (2016) of G7 leaders provided a critical approach and gave opportunity to the government of shima, Japan to frame international discussion. This was a platform to address global information and communications technology (ICT).

### **3.4.ix. International Chamber of Commerce (ICC)<sup>473</sup>**

The International Chamber of Commerce is (hereinafter referred as ICC) is a global tool with member companies spread over 130 countries. ICC facilitates Arbitration<sup>474</sup>and facilitate resolving of international disputes. It is an organization dealing with international business. International Court of Arbitration (ICC Court)<sup>475</sup> is a dispute resolution services under the umbrella if ICC, located in Paris.

ICC is an integral part of e-Commerce and has initiated policy making e-commerce projects, instruments, and services.<sup>476</sup> ICC has also led a way to Global Business Action Plan for e-Commerce. This mechanism was submitted to OECD ministers. It aimed at the development of speedy, expert-oriented mechanism for resolving of disputes in e-Commerce.

---

<sup>472</sup>Dr. S.V. Joga Rao “Law of Cyber Crimes & Information Technology Law” 226 (Publishers Wadhwa and Company Nagpur) (First Edition 2004).

<sup>473</sup>Available at [https://en.wikipedia.org/wiki/International\\_Chamber\\_of\\_Commerce](https://en.wikipedia.org/wiki/International_Chamber_of_Commerce) (Last visited on March 26, 2019).

<sup>474</sup>Available at <http://internationalarbitrationlaw.com/about-arbitration/international-arbitration/institutional-arbitration/international-chamber-of-commerce-icc-international-court-of-arbitration/> (Last visited on March 26, 2019).

<sup>475</sup>Yun Zhao, “*Dispute Resolution in Electronic Commerce*” 64 (Volume 9) (MARTINUS NIJHOFF PUBLISHERS, LEIDEN/ BOSTON) (Printed and bound in the Netherlands).

<sup>476</sup>Yun Zhao, “*Dispute Resolution in Electronic Commerce*” 64 (Volume 9) (MARTINUS NIJHOFF PUBLISHERS, LEIDEN/ BOSTON) (Printed and bound in the Netherlands).

### 3.5. Conclusion

The legal issues arising in respect of the use of computers or the internet are unexplored and the laws in hand are also inefficient to decide on these matters.<sup>477</sup> The other tricky legal issue is that of protection of raw data. The person in hold of such data may even loose his right over the same, if he is not careful. In the growing trend of electronic commerce, India does not have data protection legislation to address the privacy of personal information. Wider use of internet for multiple purposes, implicates data of those going online and personal data coming into India through transborder flow does not have any protection here at all. India needs guidelines on Transborder Flows of Personal Data as that of the OECD (Transborder Flows of Personal Data 1980) to keep track of our data. Internet world calls for India to now have legislation on the protection of privacy and Data protection on an online world.

Apart from National laws, an international tool like INTERPOL is required to address the cybercrimes at an international border. Unlike Trainings conducted by INTERPOL in Australia, Argentina, Brazil and other nations, an efficient training is also required to be conducted in India to train our Police officials to handle the cyber-attack. Such training will help them in fighting a war against emerging cybercrime issues.

WTO's dispute resolution mechanism cannot access private parties and although ICC International Court of Arbitration has no problem in dealing with disputes in e-Commerce, its arbitration rules are not tailor-made for disputes arising out of the internet.

---

<sup>477</sup>Rahul Matthan, *The Law Relating to Computers and the Internet* (LEXIS Law Publishing, Charlottesville, Virginia) (Butterworths India 2000).

## CHAPTER FOUR

### REGULATORY ISSUES INVOLVED IN PROTECTION OF PRIVACY AND DATA PRIVACY IN e-COMMERCE

#### 4.1. Introduction

Information is power<sup>478</sup> when one has full control over it without the intrusion of others. With the advance of internet, distribution of individual's data and intrusions into personal space have increased over the years. An easy access to internet empowers anyone anywhere to distribute information true or false to the world and violates the privacy and misuse data of an individual.

The regulatory issue in e-Commerce is the grey area in Information Technology Act, which does not specifically provide the manner of forming a contract which takes on an online platform and untraceable jurisdiction<sup>479</sup>.

Other regulatory issue includes choice of law and choice of jurisdiction. Our legal framework on choice of law and jurisdiction were made without bearing in mind the effects of internet as such it is really difficult for regulating the changing personality of internet in e-Commerce.<sup>480</sup> Traditional style of choice of law and jurisdiction falls short of its universal application. Parties are struggling to track the location of other

---

<sup>478</sup> Peter B. Maggs et al *Internet and Computer Law* 634 (Printed in the United States of America) (2001).

<sup>479</sup>Dr. Rakesh Kumar and Ajay Bhupen Jaiswal *Cyber Laws* 95 (APH Publishing Corporation) (2011).

<sup>480</sup> Tatiana Balaban "Choice of law and Jurisdiction in E-commerce contracts with focus on B2C Agreements, available at file:///C:/Users/hp/Downloads/balaban\_tatiana.pdf (Last visited on September 9, 2019).

users in cyber space and in such turmoil it is not easy to determine the applicable law and choice of jurisdiction is another hurdle to be dealt with.

Jurisdiction is the very basis of every justice delivery system. This very basis has been threatened over the internet. In modern technological society, courts are not as free as they were in traditional society in exercising their jurisdiction over the parties to a suit. Transaction taking place in cyberspace are leaving the courts located in physical space in confusion. It is appearing to be a war between the virtual world and physical world with no comprehensive cyber laws to come in aid.

Apart from issue of choice of law and jurisdiction, question of online liability is another annoying and important regulatory issues faced by the e-Consumers and providers of information service. This issue<sup>481</sup> is a subject of debate not only in India but also in United States, U.K. and European Union. In a digital world where everything is happening online, different types of intermediaries are involved in delivering content online to end-users, making a work available over the World Wide Web. The question here is that of the legal position of these middlemen.<sup>482</sup>

Internet in e-Commerce transaction acts opposite to the concept of Jurisdiction<sup>483</sup>. Mockery of the Jurisdiction by the internet has questioned the liability of the intermediaries/ internet providers. Each Country has their own legislation to answer this question of liability of the middlemen. Questions pertaining to their liability

---

<sup>481</sup> This issue of intermediary liability may arise in different fields of law, such as trade secret law, misrepresentation, unfair competition law, product liability law, copyright law and defamation law.

<sup>482</sup> P. Bernt Hugenholtz (ed.), *Copyright and Electronic Commerce, Legal Aspects of Electronic Copyright Management* (Information Law Series-8, Published by, Kluwer Law International Ltd, Sterling House, London Kingdom) (2000).

<sup>483</sup>Niharika Vij, *Law & Technology*, 40 (Universal Law Publishing Co. Pvt. Ltd.,) (2015).

include, - to what extent the intermediaries can be held liable? And under what circumstances and situations they can be exempted? Answers to this two question depends on the circumstances of each case<sup>484</sup>.

Privacy is often referred to an interest having several dimensions, one of the dimensions being the privacy of personal data, also known as ‘data privacy or ‘information privacy’.<sup>485</sup> It is well assumed that individuals shall have legitimate claim and substantial degree of control over their data and should not be accessible to other individuals and organisation. There are underlying conflict between protecting the interest of an individual’s privacy and maintaining a fair balance of multiple competing interests.<sup>486</sup>

The regulatory issue in this chapter has been divided under the four sub-headings;-

- The first one deals with prima facie issues of security, liability of intermediaries/third party in e-Commerce transaction, choice of law, choice of forum and jurisdiction.
- The second part deals with the regulatory issues in our existing laws to deal with the privacy and data protection and
- The third part deals with these above two issues at the international level i.e. at the European Union (E.U.) and United States (U.S.).

---

<sup>484</sup> Professor H. Snijders and Professor S. Weatherill (Eds.), *E-Commerce law: National and Transnational Topics and Perspectives* (Cyril van der Net, Civil Liability of Internet providers following the Directive on Electronic Commerce), 49, (Published by Kluwer Law International) (2003).

<sup>485</sup> Nandan Kamath, *Personal Data Privacy in the Online Context, Law Relating to Computers Internet & E-Commerce, A Guide to Cyber laws & The Information Technology Act, Rules, Regulations and Notifications along with Latest Case Laws* 305 (Universal Law Publishing, LexisNexis 5<sup>th</sup> Edn., Reprint, 2016).

<sup>486</sup>*Id.*

- The fourth one deals with the International Organizations and Documents which covers the issues of privacy and Data.

#### **4.2. Regulatory issues under Domestic Law**

At the National level regulatory issues are the issues which exist in our Laws. There are no laws in our country which deals with the issues of privacy and data protection. The laws which were introduced to facilitate e-Commerce came in the form of Information Technology Act in 2000. This Act was based on UNCITRAL Model law to legalize the e-Contracts and digital signature. This Act has nowhere defined the term privacy and data privacy, which is very crucial in e-Commerce. Despite of several amendments, the latest of which was in 2008 nowhere defined these terms. Due to the inefficiency of I.T. Act, other Acts also have to deal with the issues of privacy and data protection but still they lack in curbing these issues.

Code of Civil Procedure, 1908, Indian Penal Code, 1806, Indian Contract Act, 1872, Information Technology related Acts<sup>487</sup> have been discussed below to understand the current regulatory issues in the genre of privacy and data issues in e-Commerce.

##### **4.2.i. Code of Civil Procedure, 1908 (C.P.C.)**

Code of Civil Procedure is another weapon in the Indian Legal system which under Section 20 provides for the institution of suits by the defendant or one of the defendant / (s) at the place he/she resides, or does his/her business or the place where the cause of action takes place. The issue here is there is no uniformity in the Indian laws, for instance Section 62 of the Copyright Act and Section 134 of the Trademarks

---

<sup>487</sup> “Information Technology Act, 2000 (21 of 2000)”, “Information Technology Act (Amended) Act, 2008”, “Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011” and “Personal Data (Protection) Bill, 2013”



Act, is contradictory to Section 20 of the C.P.C., and favors the Plaintiff unlike C.P.C. by allowing to file a suit at any court of the district where he /she is a resident of or place of business<sup>488</sup>. The confusion is further exaggerated by Section 13(3), (4) and (5) of the I.T. Act, 2000<sup>489</sup>.

Section 13 of the C.P.C. deals with the effectiveness of foreign judgment on Indian people.

The question on jurisdiction is mainly regarding the binding nature of foreign courts<sup>490</sup> judgments on the people of India and the binding nature of Indian judgments at an international level. A careful perusal of Section 13 of the C.P.C. makes it clear that mere error caused in the procedure in foreign court shall not affect its conclusive nature under this section as such error found in such procedure will not be considered as violation of natural justice<sup>491</sup> under section 13 (d) of C.P.C. The above mentioned six points are the only grounds for declaring foreign judgements not conclusive and apart from the listed one any other ground would make it conclusive and binding. The main focus of Section 13 of the C.P.C. is that the foreign laws should not violate the Indian laws.

The issue here is among the total population how many internet users are aware of the international laws. And how many of them are actually aware of their own laws of the Country.

---

<sup>488</sup>Prashant Mali, *Cyber Law & Cyber Crimes, Information Technology Act, 2000 with new IT Rules, 2011*, 241 (Snow White Publication Mumbai) (2012).

<sup>489</sup>*Id.*

<sup>490</sup>*Narhari v. Pannalal* AIR 1977 SC 164, *Lalji Raja and Sons v. Firm Hansraj Nathuram* AIR 1971 SC 974

<sup>491</sup>*Abdul Wazid v. Vishwanathan* AIR 1975 Mad. 261

In *Modi Entertainment Network* case,<sup>492</sup> the Supreme Court recognized that there exist no principles called non-applicability of C.P.C. in jurisdictional questions. It means that party cannot seek jurisdiction of a court even by an agreement where the court cannot exercise one and this principal extends to applicability in foreign courts too. It is an undisputed fact that by a contract, parties are free to agree to settle their disputes in a foreign court either exclusively or non-non-exclusively by ‘choice of forum’.<sup>493</sup> In another case of *Hakam Singh v. Gammon (India) Ltd.*<sup>494</sup>, the Supreme Court in *Hakam Singh v. Gammon (India) Ltd.*<sup>495</sup>, held that if there is an agreement between parties which authorize one court out of two to try the case. The agreement is valid and not against the public policy and not violates the provisions of Section 28 of the Contract Act”. Further in *Dhannalal v. Kalawatibai*<sup>496</sup>, the court reiterated legal maxims “*Ubi jus ibi remedium*” and held right come with the forum for its enforcement.<sup>497</sup>

The above cited judgments of the Supreme Court make it clear that parties are free to choose their forum and it is on the discretion of the parties to a contract to submit themselves to the jurisdiction of their choice either exclusively or non-exclusively.

#### **4.2.ii. Indian Penal Code, 1860 (I.P.C.)**

In a digital environment where buyers and sellers are meeting on virtual platform, some things are expected to go wrong. Cyber crimes are the wrongs which has occupied the concerns of every consumer around the world. It is a fact that there is no

---

<sup>492</sup> (2004) 7 SCC 447

<sup>493</sup> Available at <https://www.sconline.com/Members/SearchResult.aspx> (Last visited on August 6, 2019)

<sup>494</sup> (1971) 1 SCC 286

<sup>495</sup> (1971) 1 SCC 286

<sup>496</sup> (2002) 6 SCC 16

<sup>497</sup> Available at <https://www.sconline.com/Members/SearchResult.aspx#JP0021> (Last visited on March 11, 2019)

comprehensive law to cover all the cyber crimes. Most of the cyber crimes are discussed in length under I.T. (Amended) Act, 2008<sup>498</sup> and others are covered by I.P.C 1860. Section 378, 403, 405 and 409 of the Indian Penal Code engages itself with providing punishment for dishonestly misappropriating the movable property for one's personal benefit, for criminal breach of trust. <sup>499</sup> I.P.C. serves as a supplementary to provisions of I.T. (Amendment) Act, 2008 and in addressing and punishing the wrong doer. For instance, for wrong -full loss or wrongful gain offender is prosecuted under sections of I.P.C. (Section 463-471), whereas for offences like data theft and hacking offender is tried under Section 66 r/w Section 43 of the I.T. Act. Prima facie it appears that there are no comprehensive laws in India to address cyber related crimes. Privacy of individuals was recognized much later in the internet age. After the commencement of I.T. Act, privacy rights of victim revenge porn were also recognized. Under section 66 E, 67 and 67 A of the I.T. Act these victims can file a complaint. In addition to these sections of the I.T. Act, other provisions of the I.P.C. can also be preferred to lodge a complaint. Lack of sensitisation programme to educate the consumers on cyber related issues and increased opacity in the I.T. Act accumulates the issue even further.

#### **4.2.iii. Indian Contract Act, 1872**

The Indian Contract Act of 1872 provides for protection of privacy of data. Like I.T. Act, it also specifies duties as well as obligations of the parties involved in a contract regarding its use and processing of a data. The importance of Contract Act is it binds

---

<sup>498</sup> NS Nappinai, Cyber Laws Part II: A guide for victims of cyber crimes, *available at* <https://economictimes.indiatimes.com/tech/internet/do-you-know-how-to-report-a-cyber-crime-heres-a-guide-for-victims/articleshow/61464084.cms?from=mdr> (Last visited on 24/09/2019 at 2:35 PM).

<sup>499</sup>Jayanti Ghosh and Uday Shankar "Privacy and Data Protection Laws in India: A Right-Based Analysis" *Bharati Law Review* (65-66) (2016).

parties to a contract to protect the data as per the agreed terms and conditions relating to its use and process.<sup>500</sup>

A man of ordinary prudence would believe that a contract would be binding on every individual the same way irrespective of their jurisdiction and Nationality. They are under the false impression that their State laws would be applicable to resolve all the issue taking place across the globe. They are unknown of the fact that each country has their own governing laws and are binding to their own subjects only. They are too naive to know that rightful act committed in one country might violate the law of another.

Contract between two parties in cross border were not recognized neither in domestic laws nor in private international laws. In pre-internet age people hardly engaged themselves in any forms of contract. Businesses were conducted either on barter system or face values. The advent of internet age complicated everything. As people have started to conduct their businesses online, their protection has become a concern like never before. Consumer protection concerns have crossed the national borders as they are in e-contracts at international platforms in e-Commerce.

These fast ongoing transactions between the consumers on internet are not easy to be dealt by any law, as there is no uniformity in cyber laws. Traditional method of contract law is not at all proficient in guiding the e-Contracts. As a consequence of inefficiency in both legal and regulatory level, it is the e-consumers who are facing the problem at large. The Indian Contract Act, 1872 deals with contract among the

---

<sup>500</sup> Latha R. Nair. "Data Protection efforts in India: Blind leading the Blind?" *NLSIU Bangalore, Indian Journal of Law and Technology* (2) (2008).

people on physical platform whereas Section 11 of the UNICTRAL Model law on e-Commerce deals with contract which takes place on virtual platform. Section 11 is regarding the formation and validity of contracts.<sup>501</sup>

#### **4.2.iv. Information Technology (Amendment) Act, 2008**

The Information Technology (Amended) Act 2008 has inserted provisions relating to the 'data protection'. Section 43 A & 72 A of the said Act talks about the protection of the same. Information Technology Act, 2000 defines both the term 'data'<sup>502</sup> and 'computer data base'<sup>503</sup>. Section 2 (0) of the Copyright Act, 1957 also provides that unless the context otherwise requires, literary work includes computer program, tables and compilations including computer databases. Thus, the Copyright Act, 1957 also provides protection to data property<sup>504</sup>.

The issue is that the expression 'data privacy' has nowhere been defined neither by the Information Technology Act, 2000 nor the Information Technology (Amended) Act, 2008. Section 1 (2) read with Section 75 of the Act, provides long arm jurisdiction and if a person (including a foreign national) contravenes the data and privacy rights of an individual by means of computer, computer system or computer

---

<sup>501</sup> A. Mohamed Mustaque "Online Dispute Resolution with Special Emphasis on Mediation in India" (2012) 4 SCC J-7, available at <https://www.sconline.com/Members/SearchResult.aspx> (Last visited on September 9, 2019)..

<sup>502</sup>Section 2 (1) (o) . "data".-means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been processed in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, may be in any form (including computer printouts, magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;

<sup>503</sup>Section 43. Explanation .- The expression computer data base means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalized manner or have been produced by a computer, computer system or computer network and are intended for use in a computer system or computer network.

<sup>504</sup> Nandan Kamath, *Personal Data Privacy in the Online Context, Law Relating to Computers Internet & E-Commerce, A Guide to Cyber laws & The Information Technology Act, Rules, Regulations and Notifications along with Latest Case Laws* 305 (Universal Law Publishing, LexisNexis) ( 5<sup>th</sup> Edn.),( Reprint, 2016).

network located in India, he would be liable under the provisions of the Act. The issue in the current Act [Information Technology (Amended) Act, 2008] in hand is that the Act does not address the liabilities of intermediaries /mid-man. Here the question is where on earth the aggrieved will sue the intermediaries on violation of his/her right. Another issue is that of unauthorised access which directly violates the privacy rights of the owner. Computer tampering, computer hacking violates the data and privacy right of the owner. The issue that concerns everyone is that a network service provider will not be liable in an action for damages if he/she proves her innocence.<sup>505</sup>.

#### **4.2.v. Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011<sup>506</sup>**

Section 43A<sup>507</sup> and 87 (2)<sup>508</sup> acts as the guiding torch in India but are not comprehensive in tackling the issues of privacy and data protection in e-Commerce platform. Although some of the key words like personal information, password, sexual orientation, biometric information, medical records and history of bank details and physical & physiological information were identified to be of sensitive personal information by this Rule of 2011, it excluded that information to be of sensitive nature which is freely available in the public domain.

The drawback of this Rule of 2011 is it lacks behind the definitions provided by other Nations around the World. Like I.T. (Amended) Act, 2008 this Rules also lays down certain requirements to be adhered by the Body Corporate in course of dealing with

---

<sup>505</sup> I.T. Act, 2000 (Act 21 of 2000) , s.85.

<sup>506</sup> Reasonable security practices and procedures and sensitive personal data or information Rules, 2011

<sup>507</sup> Information Technology Act, 2008

<sup>508</sup> Reasonable Security Practices and Procedure and Sensitive Personal data or information Rules, 2011

the process like collection of sensitive information, access of those information and as well as with drawl of the same. Here the issue is this rule does not provide the number of requirements which are to be implemented and compiled by the Body Corporate. In addition, there is no clarification as to the provisions of privacy policy, its application regarding the notice which is to be provided for the same. Another loophole in the rule is that Rule 5 (Collection of Information) and Rule 6 (Disclosure of Information) do not separately bound the Body Corporate located outside India<sup>509</sup>.

The only positive trait of this rule is it prohibits publication of sensitive personal data or information and its disclosure to unauthorized third party including Government agencies<sup>510</sup>.

#### **4.2.vi. Personal Data (Protection) Bill, 2013** <sup>511</sup>

Beside Information Technology Act, India has Personal Data (Protection) Bill of 2013. The main aim of this Bill appears to veil the identity of the data subject. This Bill has defined personal data, biometric data, sensitive personal data, data processor as well as the data subjects. The manners in which data are to be processed and regulated are all prescribed in this Bill. Further the collection of data and requirement of obtaining prior ‘consent’ from the data subject has also been taken care of. Conditions for obtaining data without prior consent from the data subject have also been given in this Bill, such conditions includes national emergency, national security and prevention, prosecution and investigation of cognizable offences. Transfer of personal data for processing from data controller to data processor which can be

---

<sup>509</sup>Peter B. Maggs, John T. Soma, *et al.*, *Internet and Computer Law* 634 (2001) (Printed in the United States of America).

<sup>510</sup>*Id.*

<sup>511</sup> The Personal Data (Protection) Bill, 2013 *available at* <https://cis-india.org/internet-governance/blog/the-personal-data-protection-bill-2013> (Last visited on September 24, 2019).

within India or otherwise has also been arranged under this Bill. Security and confidentiality of data are another prime concern.

#### **4.2.vii. Information Technology (Intermediaries Guidelines) Rules, 2011**

India does not have any laws on ‘privacy’ and ‘data’ protection, but efforts have been made in the past by the advocates for the protection of ‘privacy and data’.

It is pertinent to mention here the 2011 reports of experts on privacy i.e., “Personal Data Protection Bill” of 2006 and “Approach Paper for legislation on Privacy” in 2010 by the Department of Personnel and Training (DOPT). The former paper only did focus on the personal data protection, its use and disclosure, while the latter concentrated on both privacy and data protection. It was broader in concept than the former one as it also highlighted non-disclosure of personal information to unauthorized third party in the absence of consent. The motive of these papers was to recommend India for adoption of regulation on privacy and data. Both the paper pointed out the absence of culture of privacy in India along with the issue of interference of Government as well as private organization on the personal information of an individual. Such interference was in the mask of transparency and illegal marketing<sup>512</sup>.

Exemption from liability can be regarded as the loopholes in this Act.<sup>513</sup> Today one of the important issues that exist in e-Commerce is regarding the legal position of the internet service provider often referred as middlemen. In a digital network environment contents are rarely conveyed from the originator to the end users and a

---

<sup>512</sup>David J. Kessler, Sue Ross & Elonnai, “A Comparative Analysis of Indian Privacy Law and the Asia Pacific Economic Cooperation Cross –Border Privacy Rules”, *NLSIU-6* (2014).

<sup>513</sup> Na. Vijayashankar, *Cyber Laws, For every Netizen in India with Information Technology Bill 99* 155, (1<sup>st</sup> Edn. 1999), (Publishers, Ujvala Consultants Pvt. Ltd, Bangalore, India).



range of ‘providers’ act as go-betweens between content creator and consumers.<sup>514</sup> Issues of intermediary liability is not confined to only one sphere of law but extends to different fields such as trade secret law, misrepresentation, unfair competition law, product liability law, copyright law and defamation law.<sup>515</sup>

Intermediaries<sup>516</sup> are new actors on a new stage. The Internet technologies require their participation to make transaction possible. They rely on information through TCP/IP<sup>517</sup> packet switching. The issue here is that of their potential liability for third party information content of those packets. There are cases where they are easily targeted for legal action if information<sup>518</sup> content they carry infringes a third party’s right.<sup>519</sup>

Intermediaries providing service on internet mainly runs two types of liability risks. The first one is that of his actions or inactions in the course of providing the service which may cause loss to a communicating user or third party. The second one is that he might be held responsible for the content of the information he has transmitted,

---

<sup>514</sup> Kamiel J. Koelman, “Online Intermediary Liability”, *Copyright Electronic Commerce, Legal Aspects of Electronic Copyright Management 7*, (Editor, P. Bernt Hugenholtz), (2000), (Published by , Kluwer Law International Ltd, London, United Kingdom).

<sup>515</sup>*Id.*

<sup>516</sup> Available at <https://blog.chavannes.net/wp-content/uploads/2017/05/Intermediary-liability-IvIR-2017.pdf> (Last visited on December 9, 2019).

<sup>517</sup> TCP/IP is short for Transmission Control Protocol/Internet Protocol. TCP/IP is the suite of communications protocols used to connect hosts on the Internet. TCP/IP uses several protocols, the two main ones being TCP and IP, Vangie Beal, “TCP/IP”, available at [https://www.webopedia.com/TERM/T/TCP\\_IP.html](https://www.webopedia.com/TERM/T/TCP_IP.html) (Last visited on December 9, 2019).

<sup>518</sup> Although these intermediaries operate via software which processes information automatically and in ignorance of its content or the nature of the transaction and in ignorance of its content or the nature of the transaction, they are legally targeted. The originator of the offending information content has insufficient access to pay substantial damages (the ‘deep pocket’ concept).

<sup>519</sup> Chris Reed *Internet Law* 90 (Edn. 2nd) (First Published 2004, Reprint 2005, First Indian Reprint) (Published by Universal Law Publishing. Co. PVT.Ltd.).

either being forced to pay compensation to the person aggrieved by the content, or even committing a criminal offence.<sup>520</sup>

### Limitation on intermediary liability

The liability of the internet intermediaries is one of the issues of crucial importance. The limitless internet boundaries sets a differing liability models across national boundaries which creates uncertainty for intermediaries as to the scope and extent of their potential liabilities which in turn acts as a major discouragement to market entry or the provision of new services. The drawback of the I.T. Act is, Section 79 is an exception to penalizing intermediaries which allows the internet service providers to easily escape their liability simply on proving 'due diligence'.<sup>521</sup>

A need for limitation on liability of the internet liability was felt on many occasions and for many legal reasons over the time. There are areas where liability issues present real and intractable barriers to intermediary activity;

- New services, such as the identification of internet actors, where the geographical and jurisdictional diversity of recipients makes the assessment of liability impossible.
- Liability for third party content.

There is a growing international consensus that in order to solve this problem in respect of third party content liability<sup>522</sup>, intermediaries should be freed from liability

---

<sup>520</sup> *Id.*

<sup>521</sup> Prashant Mali, *Cyber Laws & Cyber Crimes, Information Technology Act, 2000 with New I.T. Rules, 2011*, 247 (Snow White Publications Pvt. Ltd., 2012).

<sup>522</sup> Declaration of the Bonn Ministerial Conference on Global Information Networks 6-8 July 1997:-

41. Minister underlines the importance of clearly defining the relevant legal rules on responsibility for content of the various actors in the chain between creation and use. They recognize the need to make a clear distinction between the responsibility of those who produce and place content in circulation and that of intermediaries.

by granting them immunity.<sup>523</sup> Unlike European Countries, non –European Countries like India do not have any laws specifically allowing for restrictions on transborder flows of personal data.<sup>524</sup>

### **4.3. Other Regulatory issues at Domestic Level**

The first and the foremost regulatory issue discussed in statement of problem of my first chapter includes issues of security, issues of liability of intermediaries in e-Commerce transaction, issues of choice of law, choice of forum and jurisdiction in e-Commerce. These issues are discussed as follows;-

#### **4.3.1. Issues of security in e-Commerce**

The legal issue of privacy rights in e-Commerce have dwindled the users faith in electronic mode of transactions. Customers are occupied in e-Commerce yet reluctant for complete involvement owing to the concern for confidentiality of their data and security issues involved.<sup>525</sup>

#### **4.3.2. Issues of liability of intermediaries in e-Commerce transaction**

There are two types of intermediaries, (i) internet access and (ii) service provider (ISP).The scope of immunity of service provider has been laid down in the case of *Google India Private Limited v Vishaka Industries and Others*.<sup>526</sup>

---

42. Ministers stress that the rules on responsibility for content should be based on a set of common principles so as to ensure a level playing field. Therefore, intermediaries like network operators and access providers should, in general, not be responsible for content. This principle should be applied in such a way that intermediaries like network operator and access provider are not subject to unreasonable, disproportionate or discriminatory rules. In this case, third-party content hosting o

<sup>523</sup> Chris Reed *Internet Law* 122 (Edn. 2nd) (First Published 2004, Reprint 2005, First Indian Reprint) (Published by Universal Law Publishing. Co. PVT.Ltd.).

<sup>524</sup>Lee A. Bygrave *Data Protection Law, Approaching Its Rationale, Logic and Limits* 80 (Edtr. Prof. P. Bernt Hugenholtz) (Kunwar Law International, The Hague, London, New York)(2002) .

<sup>525</sup>Talat Fatima, “Cyber Crimes” 274-275 (EBC Publishing) (2016).

<sup>526</sup> 2019 SCC OnLine SC 1587

### 4.3.3. Issues of choice of law in e-Commerce

Choice of law and jurisdiction in e-Commerce is one of the toughest questions to be decided by the Court. A court can adjudicate upon a case effectively only if it has the jurisdiction. When a matter involves questions like choice of law and jurisdiction in e-Commerce, determination of applicable law is very important. With different countries having different laws, how the question of choice of law and jurisdiction are to be decided. Different countries will have different judgements on the same issue. Court can determine its jurisdiction and apply law only on physical location but how can it apply its jurisdiction in cyberspace. Internet users are everywhere belonging to different countries having their own laws and such laws are based on their national interest. Disputes in e-Commerce involve persons of different countries therefore determination of one applicable law is very difficult. ‘Choice of law’ is a crucial question in this digital era with no answer. Many scholars over the years have debated this issue and have suggested for having a separate law on cyberspace i.e. *lex cyberalty*. Uniformity in cyber law can prove to be a win-win in resolving ‘choice of law’ particularly in disputes relating to e-Commerce.<sup>527</sup>

The incorrect treatment of databases as copyright and with similar parameters shouts for having a separate law for data protection in India. Data protection is related with the concept of privacy and violation of one may obviously affect the other.<sup>528</sup> The issue of choice of law also occurs in Tort. In e-Commerce this issue is mainly seen in Intellectual Property Rights, Defamation etc. This issue is significant in tort as cyber tort mainly occurs in the absence of contract between the parties.<sup>529</sup> Litigation is a

---

<sup>527</sup> Yun Zhao, *Dispute Resolution in Electronic Commerce*, 124-127 (Martinus Nijhoff Publishers).

<sup>528</sup> Jayanti Ghosh and Uday Shankar “Privacy and Data Protection Laws in India: A Right-Based Analysis” *Bharati Law Review* 58 (2016).

<sup>529</sup> Yun Zhao, *Dispute Resolution in Electronic Commerce*, 141 (Martinus Nijhoff Publishers).

weapon for deciding upon a conflict. This weapon of the Court has been threatened with the issue of ‘choice of law’ and ‘jurisdiction’. Internet is the reason in these modern eras, which have questioned the traditional method of proceedings across the globe.<sup>530</sup>

In the event of legal problem in e-Commerce ‘choice of law’ by the parties to contract is one of the most annoying one. In a borderless cyberspace lawyers are often struggling with choosing the correct law. Choosing a proper clause in choice of law plays a very crucial role in a contract between two parties of different nations.<sup>531</sup>

#### **4.3.4. Issues of Choice of Forum in e-Commerce**

Choosing a forum is easy, when parties involved in a traditional transaction are from different jurisdictions and are also easy to be governed by the laws of the country. The party to disputes, only need to decide upon which law of the country shall govern the transactions so performed. The theory of functional equivalence applies to treat this form of transactions. The issue of choice of forum is difficult in e-Commerce as the theory of functional equivalence is difficult to apply as that of in land. The traditional law of jurisdiction fails when transactions are carried out over the internet. The activities which may be lawful in one country may oppose the law of another country. Indian Courts can grant injunction to only those party in an appropriate case, where it can exercise its personal jurisdiction. Jurisdiction *in personam* can only be exercised to the people upon whom the court has jurisdiction and should not interfere with the jurisdiction of another court.<sup>532</sup> The issues in e-Commerce, is parties in online

---

<sup>530</sup>*Id.* at 151.

<sup>531</sup> The Choice of law clause in contracts between parties of developing and developed Nations, available at <https://pdfs.semanticscholar.org/7a9e/271fdd141c9daaeb72ed985e97668ab8c88.pdf> (Last visited on September 9,2019).

<sup>532</sup>Rakesh Kumar and Ajay Bhupen Jaiswal, *Cyber Laws* 64 (APH Publishing Corporation, New Delhi) (2011).

activities do not know with whom they are doing business, and where do they reside. In the event of any fraud or wrong, parties are clueless as to which forum to choose and against whom.

#### **4.3.5. Issues of choice of Jurisdiction in e-Commerce**

Unlike physical world, cyber world lacks boundaries and borders. As such it is an admitted fact that it is really a difficult task to frame laws for governing the cyberspace. Till date no single State has been successful in framing law to exercise control over the internet. Due to lack of physical boundaries the consequences arising are more threatening as compared to in the physical world. The difficulty is also in deciding about which State will have jurisdiction to frame cyber law and which State shall adjudicate a cross border dispute. This is a question which every Nation is facing at this moment. Some of the eminent scholars like Johnson and Post have made a remark on the decreasing significance of one's physical stand in cyberspace by pointing that increase in online activities is decreasing importance of geographical border in cyberspace, thus affecting the control over people in their online activities.<sup>533</sup>

Jurisdiction divides the power of one country with that of the other, whereas on the other hand Internet knows no boundaries. As e-Users engage themselves in online activities there is an involvement of at least three jurisdictions<sup>534</sup>. The issue here is the absence of uniform and internationally recognized laws having a universal

---

<sup>533</sup> Karnika Seth, *Computers, Internet and New Technology Laws, A Comprehensive reference work with a special focus on development in India* (LexisNexis) (2013).

<sup>534</sup> It involves the laws of a State/Nation of such users, the laws of the State/Nation where the transaction takes place and third the law which applies to the person or business with whom the transaction takes place.

Prashant Mali, *Cyber Law & Cyber Crimes, Information Technology Act, 2000 with new IT Rules, 2011*, 3 (Snow White Publication Mumbai, 1<sup>st</sup> Edn.) (2012).

application. Problems related to cyber are invited when medium of internet do not understand the limit and sovereignty<sup>535</sup>.

The issue of 'Jurisdiction' has not secured India. The I.T. Act, 2000 has been debated and questioned numerous times over jurisdictional issues. One of the questions is regarding the involvement of parties of different jurisdictions, where person/(s) of one jurisdiction wants to sue another. The confusion is of two areas viz; the defendants residence and the place where cause of action arises<sup>536</sup>.

International trade flourishes only when there is a free flow of personal data in cross border. The issue is not in the free flow of data but the issue of lack of appropriated safeguards. The situation is not threatening when data flows between two member states. The issue of privacy and data privacy is threatening only when there is an involvement of third Countries and lack of comprehensive laws to deal with the issue<sup>537</sup>.

David R. Johnson and David Post are the prominent scholars who have pointed out the issue of jurisdiction in e-Commerce. According to them the problem lies in deciding between what is real and what is unreal in online world as unreal nature of people often appears to be real. Another issue highlighted by them in e-Commerce is the tracing of the activities which takes place regardless of boundaries.<sup>538</sup>

---

<sup>535</sup>*Id.*

<sup>536</sup>*Id.* at 241.

<sup>537</sup> Diane Rowland, Uta Kohl, *et. al.*, *Information Technology Law*, 162 (British Library Cataloging in Publication Data, 4<sup>th</sup> Edn.)(2012).

<sup>538</sup>Yee Fen Lim, *Cyberspace Law*, 68 (Oxford University Publication) (2008).

Jurisdiction is basically power of any Court to decide upon a dispute or to hear the case and deliver a judgment. Jurisdiction in a traditional way is usually divided into two, one is the subject matter jurisdiction and two is the personal jurisdiction. The issue of jurisdiction begins the moment when activities of illegal nature are carried out over the internet. It is very difficult to trace the geographical limitation and exercise jurisdiction by the Court. In the absence of jurisdiction Court can not try an offender who is a subject of different jurisdictions. Yahoo<sup>539</sup> is a well-known case in the genre of jurisdictional conflict. The fact of these case states that Court directed Yahoo! to remove links and all materials from its websites pertaining to Neo Nazism and despite of the order being challenged on the ground that it violated the U.S. Constitution's first amendment, Yahoo, had to remove all the contents as directed by the order. This case is one of the most important cases in the history of jurisdiction because it was for the first time that a foreign court had exercised its preliminary jurisdiction to decide a case not located within its physical boundaries<sup>540</sup>.

Indian Courts have also interpreted Section 75 of the I.T. (Amendment) Act and Section 20 of the C.P.C. in number of cases<sup>541</sup> on issues of extraterrestrial jurisdiction. For instance in *Banyan Tree* case<sup>542</sup>, the question before the single judge was regarding its jurisdiction to entertain the case. After careful analysis of the facts of the case, the Delhi High Court also highlighted on intention of the wrong doer in “purposefully availing”<sup>543</sup> of the jurisdiction of the U.S. Court in other cases<sup>544</sup> on

---

<sup>539</sup> 2001 Us Dist. LEXIS 18378 (N.D. Cal. 2001) & 145 F. Supp.2d 1168 (N.D. Cal. 2001)

<sup>540</sup>Dr. Amita Verma, *Cyber Crimes and Law*, 318,323 (Central Law Publications) (2009).

<sup>541</sup>*Casio India Co. Ltd. v. Ashita Tele Systems Pvt. Ltd.* 2003 Del, *India TV v. India Broadcast Live*, 2007 Delhi HC, *IPRS v. Sanjay Dalia*, 2008 Delhi HC.

<sup>542</sup> (2009) SCC OnLine Del 3780

<sup>543</sup>*International Shoe Co. v. Washington* 326 U.S. 340 (1945), available at <https://www.sconline.com/Members/SearchResult.aspx> (Last visited on November 26, 2019)



jurisdictional matters and further it was averred by the Court that mere accessing of a website does not mean that Court has power to exercise the jurisdiction<sup>545</sup>.

Jurisdiction and Choice of law are the two most important issues in e-Commerce. It is not easy to address the issues of Jurisdiction and Choice of law in cyber Space as it is in physical world. With the comfort provided by the internet, the discomforts so provided are innumerable.

In e-Commerce issue of jurisdiction is much higher than in the physical world because in virtual platform jurisdiction of consumers and vendors may be scattered across the globe. This scattered jurisdiction gives rise to issues relating to choice of forum and conflict of laws.<sup>546</sup> National borders mark the jurisdictional reach of the Courts. In Online transactions jurisdictional power of the courts are questioned on its applicability.

The word 'data'<sup>547</sup> is very broad in realm covering not only the personal aspects of individuals but also the commercial aspects. The former refers to proprietary rights while the later to privacy rights. The Constitution of India protects privacy, whereas

---

<sup>544</sup>*Burger King Corp v Rudzewicz* 471 U.S. 462 (1985), *Asahi Metal Industries v Superior Court* 480 U.S. 102 (1987), *Calder v Jones*, 465, U.S. 783 (1984), available at <https://www.scoonline.com/Members/SearchResult.aspx> (Last visited on November 26, 2019)

<sup>545</sup>Prashant Mali, *Cyber Law & Cyber Crimes, Information Technology Act, 2000 with New IT Rules, 2011*, 243 (Snow White Publications Pvt. Ltd.)(2012).

<sup>546</sup> Peter P. Swire, *of Elephants, Mice, and Piracy: the international Choice of Law and the Internet* 32 (International Law 991, 1016 1998).

<sup>547</sup> Data of an individual are one's asset and are dear to him/her as they are of great significant which may be more than just a data and may be even of sensitive nature, the intrusion of which may hamper their livelihood. Such information's are to be protected and are protected vaguely by the Indian Laws like the I.T. (Amendment) Act, 2008. Taking away of such rights may violate the rights of data subject and will be illegal.

Praveen Dalal, "Data Protection Law in India: The TRIPS Perspective" (Vol. 11) March *Journal of Intellectual Property Rights*, 125-131 (2006), available at <http://nopr.niscair.res.in/bitstream/123456789/3561/1/JIPR%2011%282%29%20125-131.pdf> (Last visited at June 28, 2019).

the Indian Copyright Act, 1957 and the IT (Amended) Act, 2008 protects data. Therefore it would not be wrong to say that data are in a vague way protected under the Indian laws and lacks a proper comprehensive one to deal with the issue of data protection. There is no dispute in saying that ‘privacy’ is ones inherent personal right which shall be exercised by an individual against interference by others. It means his right to share and vice versa.<sup>548</sup>

Privacy as a concept overlaps with and relates to liberty. They are two sides of the same coin. The serious issue that lies in privacy is that of the problem of defining the essence and scope of the right<sup>549</sup>.

Right to Freedom of Speech<sup>550</sup> and Right to Personal Liberty<sup>551</sup> are some of the positive feature of our Constitution. These Articles address right to privacy as one of the fundamental right. Numerous cases<sup>552</sup> are the evidence that establishes the right to privacy in India and this right is closely related with the data protection/information of an individual.<sup>553</sup> In *Supreme Court of India v. Subhash Chandra Agarwal*<sup>554</sup> the Court mentioned section 2 (f) of the RTI Act, 2005, in the following words:

---

<sup>548</sup> Praveen Dalal, “Data Protection Law in India: The TRIPS Perspective” (Vol. 11) March *Journal of Intellectual Property Rights*, 125-131 (2006) 125-131 (2006).available at <http://nopr.niscair.res.in/bitstream/123456789/3561/1/JIPR%2011%282%29%20125-131.pdf> (Last visited at June 28, 2019).

<sup>549</sup> *Govind v State of MP*, (1975) 2 SCC 148

<sup>550</sup> The Constitution of India, art.19(1) (a).

<sup>551</sup> The Constitution of India, art. 21.

<sup>552</sup> *R. Rajagopal v State of Tamil Nadu* AIR 1995 SC 264; *Sharda v. Dharampal*, AIR 2003 SC 3450; *District Registrar and Collector v. Canara Bank*, (2005) 1SCC 596; *State of Karnataka v. Krishnapa* AIR 2000 SC 1470; *State v. N.M.T. Joy Immaculate*, AIR 2004 SC 2282; *X V. Hospital Z* AIR 1999 SC 495; *Kottabomman transport Corporation Limited v. State of Travancore and others*, AIR 1992 Ker. 351; *Registrar and Collector, Hyderabad and Anr. V. Canara Bank Etc* AIR 2004 SC 935.

<sup>553</sup> Available at <https://www.sconline.com/Members/NoteView2014.aspx?citation=JTXT-0002123879&&&&40&&&&Search&&&&fullscreen> (Last visited on June 28, 2019).

<sup>554</sup> 2009 SCC OnLine Del 2714 : (2009) 162 DLT 135 : (2010) 1 Kant LJ 383 : (2009) 82 AIC (Sum 13)

“information” which means “any material in any form, including records, documents, memos, e-mails, opinions, advices, press releases, circulars, orders, logbooks, contracts, reports, papers, samples, models, data material held in any electronic form and information relating to any private body which can be accessed by a public authority under any other law for the time being in force”.<sup>555</sup>

In *Ram Jethamalani & Ors v. Union of India*,<sup>556</sup> the apex Court explicitly uttered about ‘right to privacy’ as a scripted rights.<sup>557</sup> In India only few laws are applicable to the entire Country. One of such law having applicability to all States of India is the I.T. Act, which was passed in the year 2000. Jurisdiction under this Act is a prescriptive one. Its jurisdiction is limited by international law.<sup>558</sup> This Act states that offences committed outside India by any individual shall be punished as per this Section if the offence involves use of a Computer, Computer System or Computer Network located in India.<sup>559</sup> The issue in this Section and Act as a whole is its ineffectiveness. It is a well known fact that ‘Internet’ travels across every jurisdiction and it would be unfair to punish a person under this Act for offences which includes use of a Computer located in India. It would be totally unfair and gross because a computer located and used in India might host a content located in foreign Country and such content may only be legal in that foreign Country and illegal in India. In

---

<sup>555</sup>Jeet Singh Mann, *Strengthening the mission of Right to Information in India*, available at <https://www.scconline.com/Members/SearchResult.aspx> (Last visited on August 10, 2020).

<sup>556</sup> (2011) 8 SCC 1

<sup>557</sup> The advocates of right to privacy conceive this right as having many dimensions. History often speaks of having a paradigm shift in its notion from media, territorial, communication and bodily privacy. Among them ‘information privacy’ is the latest creation of internet and was defined by Westin in 1968, available at <https://arxiv.org/ftp/arxiv/papers/1505/1505.07683.pdf> (Last visited on June 28, 2019).

<sup>558</sup> Jurisdiction under the Information Technology Act, 2000 available at [https://shodhganga.inflibnet.ac.in/bitstream/10603/7829/14/14\\_chapter%205.pdf](https://shodhganga.inflibnet.ac.in/bitstream/10603/7829/14/14_chapter%205.pdf) (Last visited on September 23, 2019).

<sup>559</sup>Section 76 Clause (2).

such circumstances the question would be can a person be tried in Indian Courts for choosing to view a site which is considered to be illegal in India on a computer located within its jurisdiction ? Another issue is regarding its applicability in foreign lands<sup>560</sup>.

It might appear easy as per the theory of functional equivalence which holds that on-line position should be taken care of in the same way as it would be treated off-line.<sup>561</sup> Somehow this approach is correct as it is the same natural people who are engaged in online transaction in the same way as they would engage themselves in physical platform. Law per se is applicable equally to every person if they are the subject of the same country or who falls within the ambit of same court's jurisdiction. But the issue in virtual world is that of the multiplicity of players. There is no problem if two individuals of different countries are engaged in a single transaction. The issue pops up only if there is a breach of contract and the issue has to be decided as per the applicable law.

Parties who are subjects of the same Country belonging to different jurisdiction divided by their personal territory resolve their issue by agreeing upon the place of instituting their matter according to their governing law. The case is not so in e-Commerce, as internet knows no boundaries and it knows no law. Internet knows no limitation and do not consider the trouble of jurisdictional conflicts. This insensitive nature of the internet has given a headache to many law makers, advocates of privacy and Data and scholars across the globe. The research gap in privacy and Data Protection with that of the issues of choice of law and jurisdiction is endless.

---

<sup>560</sup>Dr. Amita Verma, *Cyber Crimes and Law*, 324 (Central Law Publications) (2009).

<sup>561</sup>Rakesh Kumar and Ajay Bhupen Jaiswal, *Cyber Laws*, 48 (APH Publishing Corporation, New Delhi) (2011).

While exercising jurisdiction over the internet, court looks into the totality of the circumstances to have a better insight of the activities of the individuals involved in internet.<sup>562</sup> Jurisdiction of Indian courts over the activities performed online is covered by I.T. Act, 2000. This Act under clause (2) of section 1 states that, it shall also be enforceable and extended to offences committed by person outside the territory of India. However, this section and Act in toto do not makes it clear regarding how it shall be applicable to offences so committed outside India. With the growing online activities in cyberspace, the traditional method of determining jurisdictional boundaries is shrinking at a speed.<sup>563</sup>

Unlike other eminent Jurist, who supports the theory that territorial jurisdiction cannot be applied in cyberspace, Dr. Talat Fatima, Principal of Government Law College, on the other hand believes that as long as internet is accessible by the people, as long as they log in, it would not be true to say that territorial jurisdiction cannot be extended to virtual world. According to her, this notion fails only because of the legal hardship in dealing online activities and incapacities of regulatory regimes.<sup>564</sup>

#### Personal Cyberspace Jurisdiction

Courts exercise its jurisdiction only where it is enforceable. Personal Cyberspace jurisdiction is confined to the applicability of court's jurisdiction over a particular subject/s. Determination and applicability are the two keys to consider in Personal Cyberspace Jurisdiction. 'Physical presence' is the essential criteria upon which a court relies on while determining its Personal jurisdiction. In Personal cyberspace

---

<sup>562</sup>Dr. Amita Verma, *Cyber Crimes and Law*, 338 (Central Law Publications) (2009).

<sup>563</sup>*Id.* at 432.

<sup>564</sup>Dr. Talat, *Cyber Crimes* 41 (EBC Publishing (P) Ltd.) (2016).

jurisdiction, the court first figures out the difference between resident and non-resident as only on its subject it can exercise its jurisdiction.

In traditional Society, Countries are exercising jurisdiction only within its territorial limits. But the case is different in US, as powers of the applicable courts with respect to cause of action are considered in determining the jurisdiction. ‘*Minimum contacts*’ is the approach followed by the US courts according to which even a ‘*minimum contact*’ with the forum state would suffice to attract the jurisdiction over non-state actors.

When internet and e-Commerce is happening globally in tandem, our traditional legal system appears inefficient. However in US, they exercise extraterritorial jurisdiction and long arm statutes which empowers court’s jurisdiction over non-resident defendants.<sup>565</sup> Two perspectives have been preferred to evaluate “*cross-border issues*”; “*prescriptive*” and “*enforcement*”.<sup>566</sup> The former illustrates the State’s power to make its own law and apply accordingly to matters that comes before it. Whereas the latter speaks about the State’s dependency upon perspective jurisdiction in exercising its jurisdiction over persons or events located in different territory.

Internet has created confusion on deciding the territorial jurisdiction, which in turn is obstructing the judicial decisions in deciding a matter placed before it. Court cannot apply the same approach as it applies to physical boundaries in cyberspace. In such circumstances consumers are clueless regarding choice of forum and the Court’s

---

<sup>565</sup>*Cybersell, Inc. v. Cybersell, Inc.* (US App LEXIS 33871 1997,) *Hanson v. Denckla* (2L. Ed. 2d 1283 1958)

<sup>566</sup> Joshika Thapa, *Jurisdictional Issues in Cross border e-Commerce Disputes: A Critical Study* (2018) (Unpublished M.Phil. thesis, Sikkim University).

regarding choice of law. The issue, moreover the concern is regarding whom to sue and where to sue. Even if these questions are solved another problem is the ‘choice of law’ in cyberspace.

#### **4.4. Regulatory Issues at International Level**

The regulatory issues involved in privacy and data protection in e-Commerce is not limited to India only but extends to other countries too. As the definition of privacy differs from country to country and from one individual to another, the legal and regulatory measures also differs from country to country. Under this sub-heading issues of choice of law and Jurisdiction in US and E.U has been discussed as follows;-

##### **4.4.1.Choice of law and Jurisdictional issue in European Union (E.U.) and United States (U.S.)**

The US and the EU are the only two countries in the world to have a promising comprehensive legal setup for e-Commerce<sup>567</sup> but issues of choice of law and Jurisdiction is an unsettled issue in both United States and European Union. In US two doctrines namely the First Restatement and Second Restatement exists in addressing issue of choice of law. *Lex loci delicti*<sup>568</sup> is the rule followed by the First Restatement, while in the Second Restatement Court is normally directed to consider the significant relationship to resolve the controversy of conflict of laws.<sup>569</sup> In cyberspace, application of *lex loci*<sup>570</sup> becomes ineffective and insignificant, therefore it demands for a comprehensive International Cyber Law which would be applicable

---

<sup>567</sup> Tatiana Balaban “Choice of law and Jurisdiction in E-commerce contracts with focus on B2C Agreements. A comparative analyses of EU, US and China legal frameworks” at 8, *available at* file:///C:/Users/hp/Downloads/balaban\_tatiana.pdf (Last visited on 23/09/2019 at 2:38 PM).

<sup>568</sup> Law of the State where the Tort was Committed.

<sup>569</sup> Yun Zhao, *Dispute Resolution in Electronic Commerce*, 142-143 (Martinus Nijhoff Publishers).

<sup>570</sup> Law of the Country in which an action is brought.

to all the Countries. Such cyber laws must be able to address the issue that occurs in e-Commerce business, irrespective of where the server was located, or where the parties resides or the place from where they had accessed the internet or the law of their respective countries. Cyber laws should be uniform, certain and effective in e-Commerce.<sup>571</sup> Like US, EU also does not have any harmonized cyber laws to address the issues of choice of law. Due to absence of any conventions in EU, States were free to adopt *lex loci delicti*.<sup>572</sup> EU had been considering Rome Convention I and II for dealing with the application of applicable law with regard to issue arising out of non-contractual obligations.

After careful analysis of the existing scenario on issues of choice of law in US and EU, it appears that EU followed a more convincing approach in answering the questions pertaining to choice of law. In landmark cases of Religious Tech. Ltr. v. Lerma<sup>573</sup> and Religious Tech. Ltr. v. F.A.C.T. Net, Inc.<sup>574</sup>, U.S. courts in its judgement supported the view of giving prominence to the law of the defendant's residence. In e-Commerce it is seriously difficult to answer the questions of choice of law as anyone can do wrong from any location and such wrongful act committed in one country may not be a wrong in another.

#### **4.4.1.i. Issues of choice of law in European Union**

With the introduction of internet in human lives, issues relating to choice of law and jurisdiction have increased in almost every country if it is actively engaged in e-

---

<sup>571</sup>Yun Zhao, *Dispute Resolution in Electronic Commerce*, 143 (Martinus Nijhoff Publishers).

<sup>572</sup>*Id.* at 145.

<sup>573</sup>897 F. Supp. 260 (E.D. Va. 1995)

<sup>574</sup> 901 F. Supp. 1519 (D.Colo.1995)



Commerce with other Nation. As compared to our country, E.U. is definitely in a brighter spot with its laws which regulates the issues of choice of law and jurisdiction.

E-Commerce has become a part and parcel of E.U. too. Unlike other countries it has seen to be actively in pace in tackling the ongoing e-Commerce cross-border issues. Draft regulation to govern jurisdictional issues in cross-border consumer e-transactions was issued long time back as a promising initiative by the E.U. Commission.<sup>575</sup> As per Rome II, every seller over the internet needs to consider jurisdictional issues as well as international legislative requirements regarding the terms and conditions of contracts. E.U. has considered Rome II in favoring the laws of the country of origin of goods or services, the basis for settling disputes arising in e-business transactions. After perusing the approach of America and European one with respect to choice of law, it appears that there exists a difference between the two. In E.U. the Brussels Regulation has laid down the rules in determining the questions as to which country's courts shall have jurisdiction over the defendant. Earlier version of this Regulation was popularly known as the Brussels Convention. This Convention was the result of treaty of 1968 among the European Countries on Jurisdiction and the enforcement of judgments in civil commercial matter. As a matter of facts and record this Brussels Regulation<sup>576</sup> came to be effective on March 1, 2002, thereby replacing the Brussels Convention of 1968. Except Denmark, the rules of this Regulation of 2002 will be followed by all European countries except Denmark which is guided by the 1968 convention and EFTA Countries will follow the rules of the 1988 Lugano Convention.<sup>577</sup>

---

<sup>575</sup> Joshika Thapa, *Jurisdictional Issues in Cross border e-Commerce Disputes: A Critical Study* (2018) (Unpublished M.Phil. thesis, Sikkim University).

<sup>576</sup> This Regulation specially emphasizes on jurisdiction issues.

<sup>577</sup> *Supra* Note at 554.

#### **4.4.1.ii. Issues of choice of Jurisdiction in European Union**

The enforcement of this Act as well as the jurisdictional power of the Court<sup>578</sup> of U.K. is covered by Part 6, Chapter 12 of the Data Protection Act, of 2018. It is a clear concept that the term ‘jurisdiction’ refers to the power of the court to entertain the matter before it. The power which the court exercises on physical world is not so easy to exercise on the virtual world. The credit for this confusion roots deeply to the fast growing nature of internet.

#### **4.4.1.iii. Brussels Regulation**

To resolve Jurisdictional issues and enforcement of judgments in civil and commercial matters E.U came up with the Brussels Regulation. This regulation even extends to online commercial disputes. This Convention authorizes the court to hear the case irrespective of nationality if domiciled in Contracting State. E.U. has also established a competent jurisdiction in each of the member States<sup>579</sup> through the ‘the Brussels Regulation.’<sup>580</sup> To raise a claim e-user must ensure that the court to which it intends to go has a jurisdiction to entertain that particular issue.

#### **4.4.1.iv. Issues of choice of Law in United States**

Choice of Law is synonymous to conflict of laws. It occurs when two different laws are involved and when there is a difference between two different legal jurisdictions.<sup>581</sup> The issue is how to locate customers in digital platform. U.S.A is

---

<sup>578</sup> Jurisdiction of Courts under Chapter 12 of the Data Protection Act, 2018

<sup>579</sup> Art.1.1. “This Regulation shall apply in civil and commercial matters whatever the nature of the court or tribunal.3. In this Regulation, the term ‘Member State’ shall mean Member States with the exception of Denmark”. Example cases: *LTU v. Euro control* (1 CMLR 293 1997), *Netherlands State v. Ruffer* (3 CMLR 293 1981).

<sup>580</sup> Council Regulation (EC) No.44/2001, of 22 December 2000.

<sup>581</sup> Choice of Law, available at [https://en.wikipedia.org/wiki/Choice\\_of\\_law](https://en.wikipedia.org/wiki/Choice_of_law) (last visited on November 28, 2019).

burden with this issue at two levels. One is Inter-State and another is at international level. In U.S.A. there are 50 States in total and each of these States has their own commercial laws and court system, known as Long Arm Statute.<sup>582</sup>

#### **4.4.1.v. Issues of choice of Jurisdiction in Unites States**

The extra territorial implementation of the U.S. laws solely depends on two factors. Firstly, the question pertains to whether a particular entity comes under the US's Court jurisdiction and secondly, the impact on its commerce and on the residents.

The Court can attain its jurisdictional power only within its national borders. The increased number of inter-jurisdictional transaction has invited issues relating to choice of law and choice of jurisdiction. The rights of the consumers to file complaints in an appropriate forum have lost its applicability in an online space. The lack of single accepted cyber laws has posed great concern in resolving the above stated issues.

If we look at U.S. approach towards choice of jurisdiction, it appears that the theory of '*minimum contacts*' is applied by the Courts having jurisdiction with regard to cause of action with a forum state. With the borderless internet, concept of jurisdictions is extended to virtual world as well. In digital platform choice of law or forum has a crucial role to play in determining the power of courts regarding its jurisdiction.

---

<sup>582</sup> Disputes, available at <https://cyber.harvard.edu/olds/ecommerce/disputes.html> (last visited on 28 November, 2019).

As jurisdiction is of two types viz; personal and extra-territorial, it becomes vital to identify its applicability in the cyber world. The former one refers to the power of the court to resolve a matter before it and identify as to whether a particular case falls within its jurisdiction or not. To exercise this type of jurisdiction a person has to be the subject i.e. has to be a resident of that jurisdiction. Concept of ‘*physical presence*’ is the key in this type of jurisdiction. The issue in determining jurisdiction owes to the default legal position of a country in exercising its jurisdiction as parties falling under its jurisdiction can only be dealt with. Whereas in case of the later one i.e. in extra-territorial jurisdiction ‘long arm statutes’ is the key in empowering the courts to exercise its jurisdiction over the non-residents defendant’s if the defendant’s contacts in the forum meet with certain statutory requirements. This jurisdictional aspect has been discussed in the case of *Cybersell, Inc v. Cybersell, Inc.*<sup>583</sup> and in *Hanson v. Denckla.*<sup>584</sup>

A jurisdictional issue in cross border is mainly looked from two perspectives, which are Prescriptive Jurisdiction and Enforcement Jurisdiction.

- a. Prescriptive Jurisdiction is regarding the State’s ability to illustrate its laws in choosing matters that comes before it. Prescriptive jurisdiction as the word suggest is itself narrow and rigid in nature, but generally its applicability involves the unlimited nature of the State to legislate any matter irrespective of the nationality of the persons involved. Information Technology Act, 2000 is the best example that provides prescriptive jurisdiction.
- b. Enforcement Jurisdiction on the other side is the State’s ability to impose laws which are applicable in the state. However the court has no jurisdiction to enforce them outside the territorial jurisdiction.

---

<sup>583</sup> (US App LEXIS 33871 1997)

<sup>584</sup> (2L.Ed.2d 1283)

Lack of boundaries in cyber world has resulted in confusion regarding applicability of court's jurisdiction which is limited to physical boundaries. In such circumstances binding nature of court's decisions are open to many criticism and debate.

#### **4.5. Principles and Guideline for privacy and data under International Organizations and Documents**

The issue of privacy and data has occupied the attention not only under the National and International Laws but in International organizations too. OECD, Hague Convention and TRIPS has been discussed to have a greater understanding. They are as follows:-

##### **4.5.1. The OECD Principles/ Guidelines on the Protection of Privacy and Transborder flows of Personal Information**

In 1980's OECD<sup>585</sup> provided measures for harmonizing national privacy legislation and for preventing interruptions in international flows of data. These principles even today are of great relevance for many states as it acts as a guiding torch for privacy protection.<sup>586</sup> There are 8 basic guiding principles meant for National application viz; The Collection Limitation Principle, The Data Quality Principle, The Data Purpose Specification Principle, The Use Limitation Principle, The Security Safeguards Principle, The Openness Principle, The Individual Participation Principle, and The Accountability Principle<sup>587</sup>.

---

<sup>585</sup> "Organization for Economic Cooperation and Development"

<sup>586</sup>Nandan Kamath *Law Relating to Computers, Internet & E-Commerce* 292 (Foreword by N.R. Madhava Menon) (Universal Law Publishing) (LexisNexis) (Fifth Edition 2012) (Reprint 2016).

#### **4.5.2. The Hague Convention on issues of conflict of law**

Conflict of law is an issue in almost every Country. There needs to have a uniform international agreement for rules in contracts. Hague Convention is one which focuses on the applicable laws for contracts which takes place at international market involving movable goods. Only five States so far has ratified this convention. This convention aims at resolving conflict of laws and further tries to unify laws in international sales.<sup>588</sup>

Article 7 (1) of the Convention recognizes the laws chosen by the parties provided such chosen laws has to be applicable to their contract as provided in Article 7(2) of this Convention. Article 8 of the convention states that in absence of choice of law by the parties, law of the seller's state shall be governed and in some case law of the buyer's state shall be applicable as per clause (2) of the same Article.

Earlier e-Commerce was not a concern of this convention mainly due to the fact that this convention is much older than the internet and e-Commerce per se.

#### **4.5.3. Trade Related Intellectual Property Rights (TRIPS) on Data Protection**

It is overwhelming to know that data and privacy as a right has also found its place as one of the essential human property which needs protection like other Intellectual properties. To name there exists four types of I.P.R.s in the world which includes, patents, trademarks, copyrights and trade secrets.

---

<sup>588</sup>Yun Zhao, *Dispute Resolution in Electronic Commerce*, 136 (Martinus Nijhoff Publishers).

As stated above there are four types of Intellectual Property Right but amendments have been brought only in the Copyright and Patents Act in order to deal with the issues in cyberspace.

While studying the issues of privacy and data protection in e-Commerce, understanding of the Copyright Act is as important as of understanding the Information Technology (I.T.) Act because Copyright Act deals with the subject matter of data. To be more precise, the Berne Convention of 1986 of protection to literary and artistic works provided that computer software, programme and compilation of data should be protected under the Copyrights Acts. Amendments have been made two times in this Act, i.e. Act No. 38 of 1994 and Act No. 49 of 1999. Section 2 (o) of this Act was amended to change and add definition to the word 'literary work' and included terms like computer programmes and computer database. Earlier to these amendments 'database' were not protected as a Copyright but today it is protected as a copyright and infringement of the same is a penal offence and also provides civil remedies<sup>589</sup> i.e. injunction damage etc. <sup>590</sup>.

In India Section 2 (o) of this Act supra<sup>591</sup> protects 'database' as literary works. The word 'database' has been substituted by Copyright Act 49 of 1999, w.e.f. 15-01-2000. Infringement of copyright is an offence in India and is defined in section 51<sup>592</sup> of the

---

<sup>589</sup>Civil remedies are provided under Articles 41-50 and 61 of the TRIPS.

<sup>590</sup> Justice Yatindra Singh, "Cyber Laws", 40-41, (Universal Law Publishing Co. Pvt. Ltd) (2007).

<sup>591</sup> Indian Copyright Act, s. 13 (1) (o)- "literary work" includes computer programmes, tables and compilations including computer databases.

<sup>592</sup> Copyright Act, s.51- When copyright infringed.— Copyright in a work shall be deemed to be infringed— (a) when any person, without a licence granted by the owner of the copyright or the Registrar of Copyrights under this Act or in contravention of the conditions of a licence so granted or of any condition imposed by a competent authority under this Act— (i) does anything, the exclusive right to do which is by this Act conferred upon the owner of the copyright, or 1 [(ii) permits for profit any place to be used for the communication of the work to the public where such communication constitutes an infringement of the copyright in the work, unless he was not aware and had no

Act. Such infringements impose criminal as well as civil liabilities on the wrong doer as already mentioned above.

Data Protection and Intellectual Property law aims at protecting databases. Indian Copyright Act, supra, U/S 63 B<sup>593</sup> speaks about infringement and liability of the wrongdoer.<sup>594</sup> Three factors determine the intellectual property of an individual, they are: labour, skill and judgement factors.<sup>595</sup>

The right of the owner of any literary, dramatic, musical, artistic and cinematographic works is recognised by law and the protection of the same is vital. Data protection and database protection prima facie appears synonymous but they are not and their protection under copyright Act is really difficult.<sup>596</sup> Data protection refers to protection of informational privacy of individuals, while database protection refers to protection of creativity.

---

reasonable ground for believing that such communication to the public would be an infringement of copyright; or] (b) when any person— (i) makes for sale or hire, or sells or lets for hire, or by way of trade displays or offers for sale or hire, or (ii) distributes either for the purpose of trade or to such an extent as to affect prejudicially the owner of the copyright, or (iii) by way of trade exhibits in public, or (iv) imports 2\*\*\* into India, any infringing copies of the work: 3 [Provided that nothing in sub-clause (iv) shall apply to the import of one copy of any work for the private and domestic use of the importer.] Explanation. — For the purposes of this section, the reproduction of a literary, dramatic, musical or artistic work in the form of a cinematograph film shall be deemed to be an “infringing copy”.

<sup>593</sup> Section 63B.- Knowing use of infringing copy of computer programme to be an offence.— Any person who knowingly makes use on a computer of an infringing copy of a computer programme shall be punishable with imprisonment for a term which shall not be less than seven days but which may extend to three years and with fine which shall not be less than fifty thousand rupees but which may extend to two lakh rupees: Provided that where the computer programme has not been used for gain or in the course of trade or business, the Court may, for adequate and special reasons to be mentioned in the judgment, not impose any sentence of imprisonment and may impose a fine which may extend to fifty thousand rupees;

<sup>594</sup> *Supra* Note 38.

<sup>595</sup> *Id.*

<sup>596</sup> The Copyright (Amendment) Act, 2012, available at [https://www.researchgate.net/publication/291354980\\_Copyright\\_Amendment\\_Act\\_A\\_Revisit](https://www.researchgate.net/publication/291354980_Copyright_Amendment_Act_A_Revisit) (Last visited on November 28, 2019).



The long ongoing plans to have law on data protection are still pending. The law on data protection must be in compliance with not only the TRIPS agreement but also with the Constitution of India<sup>597</sup>. TRIPS<sup>598</sup> agreement is far reaching and rigorous in nature as it addresses not only need for data protection but all forms of IPRs. Article 10 (2)<sup>599</sup> of the agreement recognizes protection of data<sup>600</sup>. Copyright and data protection are not same because all databases are capable of copyright protection but not all copyrightable material meet the criteria for data protection, thus there is a need to have separate law for data protection. ‘Compilation’<sup>601</sup> of data or other materials is protected under TRIPS Agreement.

#### **4.6. Conclusion**

Protection of consumer’s data and privacy has time and again been articulated by the courts in India.<sup>602</sup> Trending e-Commerce is a danger to the protection of data and privacy of consumers. There is a need for right based approach for safeguarding data privacy of an individual’s over the internet. Privacy and data privacy protection of individual in India is no where guaranteed by any law. Though right to privacy in India is developed by the judiciary on case by case basis, comprehensive law is still in need at the earliest to make all the cyber crime good. Efficient and result oriented legal and regulatory framework is needed to cure the issues of choice of law, jurisdiction and grey areas of our existing legal framework. With the growing e-Commerce our old traditional style of dealing with these issues are quite outdated.

---

<sup>597</sup> Praveen Dalal, “Data Protection Law in India: The TRIPS Perspective” (Vol. 11) March *Journal of Intellectual Property Rights*, 125-131 (2006).

<sup>598</sup> Article 9 (1)

<sup>599</sup>“Compilations of data or other material”

<sup>600</sup>TRIPS available at [https://www.wto.org/english/docs\\_e/legal\\_e/27-trips.pdf](https://www.wto.org/english/docs_e/legal_e/27-trips.pdf) (Last visited on April 30, 2019) (at 3:06 PM).

<sup>601</sup>Section 2 (o) of the Copyright Act.

<sup>602</sup>*Shakankarlal Agarrwalla v. State Bank of India*, AIR 1987 Cal 29

With trending e-Commerce concerns for e-consumers have also evolved. E-contracts plays a vital role in choice of law among the parties involved in e-Commerce as duties and obligations of the parties will be decided at first hand and the application of applicable laws shall also be easy to determine. But it is not an easy case as at least three parties from different jurisdiction is involved who are governed by three different legal systems. To conclude on which law to apply is of a huge concern. In the absence of comprehensive globally accepted cyber laws these issues will continue in circle. Choice of law and jurisdiction is trampled in e-Commerce. There is no segregation of boundaries, regions and borders. Choice of law is especially important in e-Commerce as that clause shall be binding the whole E-contract.

## CHAPTER FIVE

### COMPARATIVE STUDY OF PRIVACY AND DATA PROTECTION LAWS IN e-COMMERCE

#### 5.1. Introduction

The expansion of technology in human lives and drive in legal world is leading to the concern for privacy and data protection in this digital era. While advocating privacy protection, protection of data cannot be left at the outskirts. The laws in hand in India addressing the area of privacy and data are in the faces of Constitution, Information Technology (Amended) Act, 2008, Indian Penal Code, 1860, Code of Civil Procedure, 1908, SEBI, R.B.I. , I.P.R.s. Despite of having all sorts of laws, the legal framework in India is in need to analyze and give wholesome protection to privacy and data. Apart from National laws, right to privacy and data protection finds references in international laws and documents too. An insight of EU, U.K. AND U.S.A. Laws will give an idea to the framers and will help in framing its own complete set of laws on privacy and data protection.

The right to privacy and data protection has gained immense attention after the advancement in technology. Technology has occupied every sphere of human lives and has put under surveillance the personal and private activities of individuals. The

invasive potential of technology and computer systems has driven the demands of personal information and personal data.<sup>603</sup>

To name other central issues in e-Commerce apart from that of ‘privacy’ and ‘data protection’, are the issues of ‘choice of law’ and ‘jurisdiction’. The legislator needs to engage themselves with these two later issues efficiently and without further delay. Apart from the established laws on privacy and data protection in E.U. and U.S.A. an insight of handling mechanism of these countries on issues of choice of law and jurisdiction shall also be incorporated to understand the prevailing scenarios of e-Commerce issues in gamut.

## **5.2. Privacy and Data Protection laws in United Kingdom (U.K.)**

The year 1970 in U.K. marked the growing desire among the law makers to protect data due to the borderless growing nature of internet. Privacy protection was another concern which grabbed the attention of the U.K. legislatures. Prior to its membership with the European Union, U.K. too was struggling with its handicapped legal framework to address the issues of privacy and data protection. Information in the electronic forms which were kept by the various organisations was in danger due to the lack of efficient laws to provide security and confidentiality. The same year i.e. in 1970, a younger committee on privacy in U.K. made a recommendation on the use of computers in handling of the data. Even though the U.K. Government never considered this recommendation of the younger committee, it did result in the formation of Lindop committee on composition of Data Protection Authority. The recommendation of the Lindop committee too failed in its vision as nothing was

---

<sup>603</sup> Jayanti Ghosh and Uday Shankar “Privacy and Data Protection Laws in India: A Right-Based Analysis” *Bharati Law Review* 56 (2016).

incorporated by the then government. A momentum was finally brought by the European Convention of 1981 for the Data Protection Act of 1984. Other countries in the elite groups already had basic data protection regime and prohibited transborder flow of data to non –member groups. The threat of being left out by this elite group compelled the U.K. Parliament to frame their own.

The year 1982 and 1983 marks the struggle of U.K. to have a Data Protection Act. With the efforts in the introduction of first bill on data protection in December 1982 into the House of Lords and second bill on July 1983 finally resulted in the Data Protection Act of 1984.<sup>604</sup> U.K. has compiled its Data Protection Act of 1988 with the European Data Protection Directives (95/46/EC) which dealt with the protection, processing and free flow of data of an individual. After a decade the European Data Protection Directives (95/46/EC) was replaced by The General Data Protection Regulation (GDPR) (EU) 2016/679 which then resulted in the UK’s Data Protection Act of 2018. Processing of personal data is unlawful if it is done in contrary to the conditions laid down in schedule 2 of this Act.

Like India U.K. too have defined the terms like ‘Personal Information’ and ‘Sensitive Personal Information.’<sup>605</sup> Schedule 1, Part I of the “Data Protection Act” (DPA), UK, in its Seventh data protection principle, provides for the measures to be taken by the

---

<sup>604</sup> This Act of 1984 was introduced to provide rules of registration for data users. The Act also laid down rights of the individuals to access to that data. Part I of this Act defines “data”, “Personal Data”, “Data Subject”, “Data users” as well as provides data protection principles. Part II deals with Registration and supervision of data users, Appeals etc. Part III deals with Rights of Data Subjects. This Act was superseded by the Data Protection Act, 1988. Data Protection Act 1984, *available at* [http://www.legislation.gov.uk/ukpga/1984/35/pdfs/ukpga\\_19840035\\_en.pdf](http://www.legislation.gov.uk/ukpga/1984/35/pdfs/ukpga_19840035_en.pdf) (Last visited on November 25, 2019).

<sup>605</sup> Prashant Mali, *Cyber Law & Cyber Crimes, Information Technology Act, 2000 with new IT Rules, 2011*, 3 (Snow White Publication Mumbai, 1<sup>st</sup> Edn. 2012).

appropriate authority in the event of unauthorised or unlawful processing and damage of personal data<sup>606</sup>.

### **5.2.1.U.K.'s Younger Committee Report on Privacy, 1973** <sup>607</sup>

In United Kingdom the Younger Committee was formed under the chairmanship of Sir Kenneth Younger, with a motive to provide protection to privacy. This Committee<sup>608</sup> focused more on privacy rights than on the data protection. On the basis of the findings of this committee, personal information's held in government computers and growing intrusion into one's privacy and its threat was projected to be incorporated in the U.K.'s 'White Paper'.

'Data Privacy', 'Information Privacy' and 'Privacy' were the main area to be considered by this Committee. This Committee identified five areas causing threat to privacy. They are;

- computer's facilitating the maintenance as well as retention of data record;

---

<sup>606</sup>*Id.*

<sup>607</sup> Report of this Committee on 'privacy' was under the chairmanship of Sir Kenneth Younger. A thorough and comprehensive study was made to make this report on privacy. This report mainly focused on "To consider whether legislation is needed to give further protection to the privacy of individuals and companies against intrusions from other individuals and companies". The committee however limited their area to private sectors only. The stated focus of the report was actually recommended by the former government which was later affirmed by the succeeding government. This committee was successful by a majority of 14 to 2. Some of the focal areas of this report are as under:

- (i) Firstly, majority of the committee proposed for voluntary action and new laws for giving adequate protection in the most needed areas. This proposal invited two arguments. First argument was that it was not required to have one.
- (ii) Secondly they argued on the other hand stated that introduction of such laws might risk right of freedom of speech which is as important as right of privacy. Basically the conflict was regarding individual's right to keep his private affairs free from intrusions and rights of others to speak and write about those affairs freely which holds truth and are of public importance.
- (iii) Thirdly, the conflict was between individual's 'right to privacy' and claims of 'public interest'. The committee thought it inappropriate and even dangerous to give directions to the courts to adjudicate upon these issues. Mr. Robert Carr, Privacy (Younger Report), 13<sup>th</sup> July, 1973,

available at <https://www.theyworkforyou.com/debates/?id=1973-07-13a.1955.6> (last visited November 19, 2019).

<sup>608</sup> Peter Carey, *Data Protection in the U.K.* 2 (Published by the Blackstone Press Limited, 2000).

- easy availability of data which were accessible from different points;
- easy transfer of data;
- impractical data combination;
- Intelligible storage, processing and transmission of data.

The only major issues of this committee were on the question regarding “whether there should be general legal right of privacy?” Privacy holds an integral part in human lives. In this regard Mr. Robert Carr highlighted the importance of privacy in a society.<sup>609</sup>

Privacy in recent years undoubtedly has occupied concerns due to the unstoppable issues brought by the borderless internet. The absence of privacy as well as its presence plays a vital role in shaping the quality of life in our society.<sup>610</sup> Right to privacy is as essential as right to life, therefore it is the duty of every State to take measures for protection this right.

The grey area in this committee was only regarding its focus in private sectors as its extensive research was only confined to this sector.

### **5.2.2. Data Protection Directive (95/46/EC)**

Processing of personal data as well as free flow of data was adopted by the European Data Protection Directive (95/46/EC) on October 1995. To be a member of this EU Directives Countries were under the obligation to implement their National Laws by adhering to the prescribed data directives. Such implementations were to be done by

---

<sup>609</sup>Privacy (Younger Report), 13<sup>th</sup> July, 1973, *available at* <https://www.theyworkforyou.com/debates/?id=1973-07-13a.1955.6> (last visited November 19, 2019).

<sup>610</sup>*Id.*

the year 1998 by the member states which were at that time 24 in number. The main focus of this Directive was the protection of individual's privacy with regard to their data processing. Other aims of this Directive included the harmonization of legislation on data protection among the member states.

This Directive of 1995 has set out a paradigm for all the succeeding legislations in both U.K. and E.U. It would not be wrong to state that for the first time in world history, concerns for privacy and data protection was given immense prominence by this Directive. This directive served as a guiding torch for all the countries for framing their own laws in the field of protection privacy and data protection. The Directive in its initial stage worked on the protection of personal data in its member states and thus facilitated the transfer of personal data across national boundaries within the European Union.

Article 6<sup>611</sup> and 7<sup>612</sup> of the Directive sets out the principles to be strictly followed in processing of the data. The interesting fact of this directive is that it prohibited the use of one's data without obtaining prior permission from the owner, provided except when such act was necessary. Such processing was only to be done by obtaining the prior consent as well as satisfying the principles so laid down. Consent of the data subjects was particularly required in the special type of data such as information regarding sex life, religious views and political opinions. Right to be informed was another explicit right of the data subject under this EU Directive. Data subjects were entitled to know about the data which were collected from them or the third party and the purpose for which they were collected to be used and any other information which was deemed to be important in ensuring fair processing.

---

<sup>611</sup> Article 6 is regarding the processing of the personal data as per the established principle of the EU Directives (95/46/EC).

<sup>612</sup> Article 7 lays down the number of conditions to be satisfied at the time of processing of data.



### **5.2.3. Data Protection Act of 1984**

The first ever U.K.'s Act on Data Protection is the Act of 1984. This Act exclusively dealt with the personal data of the data subject. This Act was one of its own kinds for the first time to ever make mandatory requirements for the data holder to get themselves registered to the office of Data Protection Registrar (DPR). Criminal offences were introduced along with the compensation provisions for individuals damaged by such non-compliance as prescribed by the Act. One of the most essential principles of this Act was the processing of personal data. This principle of this legislation was enforceable only by the DPR and the Data Protection Tribunal. It was not enforceable through the courts as these principles were adopted in a continental model<sup>613</sup>.

### **5.2.4. Data Protection Act of 1998**

Prior to the Data Protection Act of 1998, United Kingdom's data regimes were looked after by the then Act of 1984. DPA of 1998 was considered to be the world's most comprehensive legislation on data protection until DPA of 2018 came into picture. The former DPA was in harmony with the European Data Protection Directives (95/46/EC). There were hardly any changes in the new Act of 1998, except changes in the definition part. New aspects of 1998 Act included the following changes:-

- enhancement in the data subject access rights;
- right of an individual to be informed of logic behind the automated decision taking;
- certain manual records which were included to in the extension of law;
- ban and conditions to be adhered to while processing of sensitive data;

---

<sup>613</sup> Peter Carey, *Data Protection in the U.K.* 4 (Published by the Blackstone Press Limited, 2000).

- ban on export of personal data to non-EEA Countries.

Under this Act, data subjects were entitled to know about their data controller's source of personal data. They had the liberty to even object on the kinds of certain processing relating to processing of direct marketing.

### **5.2.5. Data Protection Act, 2018**

U.K.'s Data Protection Act of 2018 is mainly framed on EU's General Data Protection Regulation of 2018 in short GDPR. This regulation came into force on May 25<sup>th</sup> 2018 and ensures that its data protection principles are strictly adhered to, by those who uses or deals with the personal data of other individual's. An individual under this Act have more control over its personal information and data. This Act is mainly concerned with how personal data of customers are handled by the companies etc.<sup>614</sup> GDPR applies to all of the Europe and each country have the liberty to make changes during applying the regulation. Its adaptation in U.K. resulted in the Data Protection Act of 2018, which then replaced the Data Protection Act of 1998. The growing issue of privacy and data protection is the very reason which led to the enactment of this Act.

### **5.3. Privacy and Data Protection laws in European Union**

European Union is one of the first Countries in human history to have realized the importance of privacy and that of data. Even prior to the encroachment of technology in human lives, the government of this country came up with the preventive measures to safeguard the inherent essence of human lives i.e. privacy. With regard to the

---

<sup>614</sup> What is GDPR, *available at* <https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018> (Last visited on January 30, 2020)

evolution of laws on privacy and data, important directives and Acts are discussed below;-

### **5.3.1. Data Protection Directive (95/46/EC)**

Processing of personal data as well as free flow of data was adopted by the European Data Protection Directive (95/46/EC) on October 1995. To be a member of this EU Directives Countries were under the obligation to implement their National Laws by adhering to the prescribed data directives. Such implementations were to be done by the year 1998 by the member states which were at that time 24 in number. The main focus of this Directive was the protection of individual's privacy with regard to their data processing. Other aims of this Directive included the harmonization of legislation on data protection among the member states.

This Directive of 1995 has set out a paradigm for all the succeeding legislations in both U.K. and E.U. It would not be wrong to state that for the first time in world history, concerns for privacy and data protection was given immense prominence by this Directive. This directive served as a guiding torch for all the countries for framing their own laws in the field of protection privacy and data protection. The Directive in its initial stage worked on the protection of personal data in its member states and thus facilitated the transfer of personal data across national boundaries within the European Union.

Article 6<sup>615</sup> and 7<sup>616</sup> of the Directive sets out the principles to be strictly followed in processing of the data. The interesting fact of this directive is that it prohibited the processing of personal data without the consent of the data subject, provided except when such act was necessary. Such processing was only to be done by obtaining the

---

<sup>615</sup> Article 6 is regarding the processing of the personal data as per the established principle of the EU Directives (95/46/EC).

<sup>616</sup>Article 7 lays down the number of conditions to be satisfied at the time of processing of data.

prior consent as well as satisfying the principles so laid down. Consent of the data subjects was particularly required in the special type of data such as information regarding sex life, religious views and political opinions. Right to be informed was another explicit right of the data subject under this EU Directive. Data subjects were entitled to know about the data which were collected from them or the third party and the purpose for which they were collected to be used and any other information which was deemed to be important in ensuring fair processing.

### **5.3.2. Directive on e-Commerce 2000/31/EC 8 June 2000 (ECD)**

ECD does not provide any legal definition of “Online intermediaries”. However their conduct, caching and hosting are defined in Articles 12 to 14 of the ECD. This directive under Article 4<sup>617</sup> has included the liability regulation for information society service providers (intermediaries/ Internet providers). This Section exclusively covers e-Commerce in internet market. Sovereignty of the jurisdiction of countries across the globe has been mocked by the internet which raises questions of liability of the middleman (intermediaries/ Internet providers). In the events of unlawful activities committed online with the facility of internet provided by these internet providers, can they be called upon to account for? This question has not been answered by this directive (2000/31/EC).<sup>618</sup>

Some of the objectives of this EU Directives in e-commerce are;-

---

<sup>617</sup>Directive on e-Commerce 2000/31/EC 8 June 2000 (ECD), art.4.Prohibition of prior authorisation. - Member State shall ensure that the taking up and pursuit of the activity of an information society service provider may not be made subject to prior authorisation or any other measure having equivalent effect.

Denis Sparas, EU Regulatory Framework for e-commerce, WTO Workshop, Geneva, 18<sup>th</sup> June 2013, available at [https://www.wto.org/english/tratop\\_e/serv\\_e/wkshop\\_june13\\_e/sparas\\_e.pdf](https://www.wto.org/english/tratop_e/serv_e/wkshop_june13_e/sparas_e.pdf) (last visited, November 19, 2019).

<sup>618</sup> Professor H. Snijders & Professor S. Weatherill, *E-commerce Law: National and Transnational Topics and Perspectives* (Cyril Van der Net, *Civil Liability of Internet providers following the Directive on Electronic Commerce*), 49 (Kluwer Law International, 2003).

- (i) One of the important objectives of this directive is the free movement and smooth cross-border online services.
- (ii) Legal certainty in commerce and consumers.
- (iii) Technically sound legal framework
- (iv) Fair Competition

This EU directive does not apply to these three areas viz;-

- (i) Data protection
- (ii) Tax and
- (iii) Gambling activities

Article 3 of the EU Directive does not apply to the following areas;-

- (i) IPRs.
- (ii) Consumers Contract
- (iii) Freedom of parties to choose the applicable laws.

Liability of online intermediaries:

- (i) Information society service providers exempted from their liability if third party is solely responsible for the illegal content.
- (ii) Limited liability provisions.
- (iii) Copyright and Trademark covered by the liability provisions.
- (iv)

### 5.3.3. European Union's Data Protection Act of 2018

The EU's Data Protection Bill of 2018 has 15 Chapters and 112 Sections.<sup>619</sup> This new Act of 2018 has incorporated a whole gamut of protection regime for privacy and data's of its data subject's. Provisions for Processing of personal have been incorporated by this new Act of 2018, which are mostly subjected to the GDPR.<sup>620</sup>

This Act has been adopted by number of companies to protect the privacy of its staffs and other important groups. For example; Salisbury Group Companies' has adopted the new Act of 2018 and therefore commits to protect the privacy and personal information of all its staffs, contractors as well as suppliers by ensuring safe handling of personal data by adopting lawful schemes and with sensitive attitude to justify the activities involved in handling, storing as well as processing of data in addition to other different steps so involved.<sup>621</sup>

The main area covered by this Company in the securing the privacy and data of its Netizen includes the following - Purposes of the processing, How we collect personal data, How we process personal data, Legal basis for processing personal data, Special categories of 'sensitive personal data', Legal basis for processing special categories of 'sensitive personal data', Record of processing, Sharing personal data, Retention of personal data, Security of personal data, Data Breaches, Transfer of data abroad, Automated decision making, Further processing, Right to be informed, Data subject rights, Subject Access Requests, Obligation of Salisbury Group Companies' staff and

---

<sup>619</sup>Available at <https://saveourprivacy.in/media/all/Data-Protection-Bill-Chapter-Based-Guide-Guide-12.09.2018.pdf> (Last visited on November 07, 2019).

<sup>620</sup> Part 1 of Chapter 12 of the Data Protection Act of, 2018 incorporates the protection of personal data.

<sup>621</sup> Data Protection Policy-Data Protection Act of 2018, available at [http://salisburygroup.com/sites/default/files/2018-09/Data%20Protection%20Policy%20\(Web%20Version\).pdf](http://salisburygroup.com/sites/default/files/2018-09/Data%20Protection%20Policy%20(Web%20Version).pdf) (last visited on November 07, 2019).

contractor's<sup>622</sup>, Storage of Personal Data, Use of personal data, Accuracy of personal data, Salisbury Groups' commitment to data protection and Key contacts.

This new Act of 2018 commits to protect the privacy and personal information of all its staffs, contractors as well as suppliers by ensuring safe handling of personal data by adopting lawful schemes and with sensitive attitude to justify the activities involved in handling, storing as well as processing of data in addition to other different steps so involved. <sup>623</sup>

#### **5.3.4. General Data Protection Regulation, 2018 (GDPR)**

GDPR is a modernize law for the protection of personal information of the customers of European Union. It came in the year 2018 to replace the 1995 data protection directives. This Regulation mainly came with a purpose to harmonise data protection laws across the Europe. This regulation empowers individual to control its personal information and also extends this right to a child of 16 years to give consent for processing of his/her data. GDPR also bars the automated decision making and profiling of the data subjects. Rights of the data subjects are also ensured in processing of their personal information. GDPR aims at balancing privacy and freedom of speech. <sup>624</sup>

---

<sup>622</sup> This group has entered into commitment of adhering to the Data Protection Act of 2018. The policy of this Act, covers other franchise of Salisbury Group Companies', which includes,

- Salisbury Workplace Services Limited.
- Salisbury Integrated Services Limited.
- Salisbury Engineering and Compliance Limited.
- Salisbury Security services Limited

<sup>623</sup> Data Protection Policy-Data Protection Act of 2018, *available at* [http://salisburygroup.com/sites/default/files/2018-09/Data%20Protection%20Policy%20\(Web%20Version\).pdf](http://salisburygroup.com/sites/default/files/2018-09/Data%20Protection%20Policy%20(Web%20Version).pdf) (Last Visited on November 07, 2019).

<sup>624</sup> What is the difference between the DPA, 2018 and the GDPR, *available at* <https://www.dpocentre.com/difference-dpa-2018-and-gdpr/> (Last visited on January 30, 2020).

#### 5.4. Privacy and Data laws in the United States (U.S.)

The right to privacy is not an explicit right in the United States Constitution and there is not a single principal law on the Data Protection. As per their Supreme Court rulings, there is a limited constitutional right of privacy and which subject to provisions of the Bill of Rights. This right to privacy gives protection from government surveillance, in matters relating to marriage, procreation, contraception, sexual activity, family relationships, child rearing and education.<sup>625</sup> The United States Supreme Court has addressed the right to privacy in many cases of, *Reno v Condon*<sup>626</sup>, *Kyllo v United States*<sup>627</sup>, *Watchtower Bible & Tract Society of New York, Inc., et al. v Village of Stratton et al.*<sup>628</sup>, *Board of Education of Independent School District No. 92 of Pottawatomie County et al. v Earls et al.*,<sup>629</sup> *Gonzaga Univ. v Doe*<sup>630</sup>, *Connecticut Dept. of Public Safety v Doe*<sup>631</sup>, *Doe v Chao*<sup>632</sup>, *National Archives & Records Administration v Favish*<sup>633</sup>, *United States v Flores-Montano*<sup>634</sup>, *Thornton v United States*<sup>635</sup>, *Hübel v Sixth Judicial District Court of Nevada Humboldt County et al.*<sup>636</sup>, *Illinois v Caballes*<sup>637</sup>, etc.

The data of U.S. Citizens are protected at two level i.e. federal and State levels. Firstly, there is FTC,<sup>638</sup> which is authorized by virtue of this Act to guard its

---

<sup>625</sup>Barkha and U. Rama Mohan, *Cyber Law & Crimes* 184 (Published by S.P. GOGIA (H.U.F.) (Reprint 2012-2013).

<sup>626</sup> 2000 SCC OnLine US SC 4:528 US 141 (2000)

<sup>627</sup> 2001 SCC OnLine US SC 61:533 US 27 (2001)

<sup>628</sup> 2002 SCC OnLine US SC 55:526 US 150 (2002)

<sup>629</sup> 2002 SCC OnLine US SC 75: 536 US 822 (2002)

<sup>630</sup> 536 US 273 (2002)

<sup>631</sup> 538 US 1 (2003)

<sup>632</sup> 540 US 614 (2004)

<sup>633</sup> 541 US 157 (2004)

<sup>634</sup> 541 US 149 (2004)

<sup>635</sup> 271 US 414 (1926)

<sup>636</sup> 2004 SCC OnLine US SC 55:542 US 177 (2004)

<sup>637</sup> 543 US 405 (2005)

<sup>638</sup> "Federal Trade Commission Act"



consumers against unfair or deceptive practices<sup>639</sup>. Secondly, Statutes of one State differs from that of the other. Here, privacy rights of citizens mainly include the right of the home owners to be free from drone surveillance and library records.

Data Protection laws in US is diverse in nature and lacks a general legislation. The authorities engaged with the protection of data and privacy includes, Federal Trade Commission (FTC) etc. The Consumer Financial Protection Bureau and The Department of Commerce. The most important area in which the FTC has taken initiative is the protection of privacy of consumer's and data protection. As there are no uniform data protection laws in US, the FTC has also covered areas of issues like identity theft and telemarketing under its ambit. Apart from the above mentioned restrictions, State laws also do impose restrictions on businesses that are engaged in the collection, use, disclosure of certain sensitive data viz; biometric data, medical records, email addresses, financial records, phone records, education records etc. Apart from this, the State has also come up with the laws specifically related to surveillance (for instance, drone photography & cellular location tracking). Unauthorised access, collection, transfer and processing of personal information of state's residents are also under the purview of data protection notification. A business which indulges itself with any one of the personal information of the state's residents needs to adhere itself with the data protection law even if that business lacks physical presence in a particular state. Some State even does take account of personal information's.<sup>640</sup>

---

<sup>639</sup> USA: Data Protection 2019, *available at* <https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa> (Last visited on November 11, 2019).

<sup>640</sup>*Supra* Note 639

There are few enacted laws on privacy and data in U.S.A., they are discussed below;-

#### **5.4.1. The Fair Credit Reporting Act (FCRA), 1970**

This Act was amended by another Act, commonly known as the Fair and Accurate Credit Transactions Act.<sup>641</sup> This Act requires certain types of personal information's to be securely destroyed. It also imposes restriction on Financial institutions to establish programmes i.e. Identity theft Red Flags Rule, that detect and respond to identity theft.<sup>642</sup>

#### **5.4.2. Privacy Act 1974**

The Privacy Act came in the United States in the year 1974, to maintain a fair balance between the government's need to retain information of individuals and protection of the right to privacy against unnecessary intrusion. This Act is the result of chaos in the United States in the form of surveillance and investigation of individual's by federal agencies.<sup>643</sup> This Act of 1974, protects the right of privacy in twofold, firstly it protects records held by the government agencies and secondly, it required agencies to adopt fair information practices. The issue in this Act is it does not check illegal intrusion's. This Act only covered the government sectors and there was no comprehensive privacy protection law for the private sector. This Act mainly focused on four areas which include, restriction on the disclosure of personally identifiable records maintained by agencies, individual's right of access of those information

---

<sup>641</sup>In short, FACTA.

<sup>642</sup>*Id.*

<sup>643</sup> Privacy Act of 1974, *available at* <https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1279> (Last visited on January 21, 2020).

retained by the agencies, right of the individuals to seek amendments in the agencies records etc.<sup>644</sup> Due to certain viable reasons, an amendment was made in this Act.<sup>645</sup>

#### **5.4.3. Family Educational Rights and Privacy Act, 1974 (FERPA)**

This Act in particular deals with the information related to student's record. Such record includes their records of accuracy and personal information's. Disclosure of this information is restricted without the consent of student or parents in some cases.<sup>646</sup>

#### **5.4.4. Cable Communications Policy Act, 1984**

Protection of privacy rights of an individual basically extends/includes subscribers. It's them who need greater protection. A constant engagement in the online market makes their information vulnerable. Both forms of Government supra, have framed their laws keeping in mind the privacy policy of such subscribers.<sup>647</sup>

#### **5.4.5. Electronic Communications Privacy Act, 1986**

This Act was enacted by the United State Congress in the year 1986, especially to restrict disclosure of oral or electronic communication of the employee's by the company, to protect the privacy of the employee's. The Act specifies that it is illegal to tap or capture communication on wires, unless one of the criteria is fulfilled, viz., where party has given consent or if there is a legitimate business reason or when the company needs to protect itself and an employee is free to claim their privacy policy from the company in absence of no content access policy. Unauthorised disclosure of

---

<sup>644</sup> Privacy Act of 1974, *available at* <https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1279> (Last visited on January 21, 2020).

<sup>645</sup> "Computer Matching and Privacy Act of 1988"

<sup>646</sup> *Supra* Note 639

<sup>647</sup> *Id.*

people's purchases is also held to be illegal under this Act. This act also extends the government restrictions on wiretaps to telephone calls to include transmission of electronic data by computer.<sup>648</sup> To keep a balance with the advance communication technologies, USA PATRIOT Act, clarified and updated this ECPA, 1986, whereas, ECPA updated the Federal Wiretap Act of 1968.

#### **5.4.6. Computer Matching and Privacy Act of 1988**

This Act was enacted on October 18, 1988 and came into effect on July 19, 1989. This Act was enacted to mainly establish procedural safeguards affecting agency's use of privacy records. Agencies under this Act were required to conclude written agreements specifying the terms to data subjects on data so collected. Due process rights were also given to individual's to prevent agencies from taking adverse actions.<sup>649</sup>

#### **5.4.7. The Video Privacy Protection Act (VPPA), 1988**

This Act came in the year 1988. It did not covered privacy and data issues categorically but did made provisions regarding "*wrongful disclosure*".<sup>650</sup> Therefore, it can be admitted that privacy and data related issues were handled in bit and pieces.

#### **5.4.8. The Telephone Consumer Protection Act (TCPA), 1991**

This Act regulates calls and text messages made to mobile phones. The Act further regulates residential calls which are made for marketing purposes.<sup>651</sup>

---

<sup>648</sup>ECPA, 1986, available at <https://www.sciencedirect.com/topics/computer-science/electronic-communications-privacy-act> (Last visited on January 23, 2020).

<sup>649</sup>Computer Matching and Privacy Act, 1988, available at [https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/inforeg/inforeg/final\\_guidance\\_pl100-503.pdf](https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/inforeg/inforeg/final_guidance_pl100-503.pdf) (Last visited on January 21, 2020).

<sup>650</sup>*Supra* Note 639

#### **5.4.9. The Driver's Privacy Protection Act (DPPA), 1994**

This Act of 1994, governs the privacy and disclosure of personal information of vehicle owners. Personal information's capable of identifying him/her shall be protected from being accessed illegally from the State departments of motor vehicles.<sup>652</sup>

#### **5.4.10. The Health Information Portability and Accountability Act (HIPPA), 1996**

This Act mainly covers and protects the information concerning health status, payment for health care relating to an individual. Here, Individuals can have access to a copy of their medical report on making a request to the health service provider.<sup>653</sup>

#### **5.4.11. Children's Online Privacy Protection Act, 1998 (COPPA)**

United Nation is the only country unlike India to have a well framed law especially directed towards the privacy rights of Children. It is well known as the Children's Online Privacy Protection Act of 1998. This is the first Law of U.S. dedicated towards children who are naively engaged in the internet. Due to the inevitable privacy related issues of children, the Act aimed at controlling the way in which internet service providers and web sites collected personal information of children falling under the age of 13.<sup>654</sup> Important Sections of this Act includes 1302 (1)<sup>655</sup>, 1302 (4)<sup>656</sup> and 1302

---

<sup>651</sup> *Supra* Note 639

<sup>652</sup> *Id.*

<sup>653</sup> *Id.*

<sup>654</sup> Children's Online Privacy Protection Act, 1998, available at <https://www.inc.com/encyclopedia/childrens-online-privacy-protection-act-coppa.html> (Last visited January 22, 2020).

<sup>655</sup> "child"

<sup>656</sup> "disclosure"

(8)<sup>657</sup>. Certain information's are tagged under this Act to be of personal nature, and includes, "e-mail", name of the person, address etc.

It is necessary to include the term "Parent"<sup>658</sup> under this Act, because consent has to come from them in matters relating to the information of their child.

#### **5.4.12. The Gramm Leach Bliley Act (GLBA), 1999**

This Act of 1999 was mainly framed to govern information of personal character. Segregation was made by this Act as to what information's are to be protected. It mainly covered information's rendered by financial institutions like Banks. It further made restrictions on the way information's were collected during the course of business by these institutions.<sup>659</sup>

#### **5.4.13. PATRIOT(Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism)Act, 2011<sup>660</sup>**

United State passed the Patriot Act, in the year 2011. This Act is the result of September 11, 2011 terrorist attack. The Act mainly strengthened the surveillance power of Federal law enforcement and intelligence agencies. The Act also intended to investigate and detain suspected terrorists. The Act was amended in 2003, by which changes were made in the privacy policy relating to telephone, electronic communications and operation of the foreign intelligence Surveillance Court, etc. The Act also brought amendments in the existing Wiretap Act of 1968. Computer and

---

<sup>657</sup> "Personal Information"

<sup>658</sup> section1302 (7)

<sup>659</sup>*Supra* Note 639

<sup>660</sup> "Uniting and Strengthening America by Providing Appropriate Tools required to Intercept and Obstruct Terrorism"

terrorist crimes were added as one of the serious crimes under section 201 and 202 of the USA PATRIOT Act.<sup>661</sup>

### **5.5. Privacy and Data Protection: Indian Scenario**

The concept of Right to privacy with that of data protection has gained enormous attention over the years. With the technological advancement our society has witnessed transformation both good and bad in abundance. Talking about the social transformation it is pertinent to mention that traditional society abhorred privacy and there were hardly any data to be protected. But time changed and society valued their seclusion and preferred to be left alone without interference from other fellow human beings. With the mushrooming borderless technology people became even more conscious of their data and valued privacy unlike their forefather who abhorred it.

To keep tandem with progress and safety in era of internet particularly in genre of e-Commerce, India came up with the Information Technology Act, in the year 2000 which continuous to be inefficient despite of several amendments. Change is necessary for any society to progress but the change brought by the internet in the lives of people has invited greater risks. Such risks have appeared in the forms of infringement of privacy, data theft, issue of choice of law, jurisdiction etc. The misfortunate brought by internet is enormous and has ruined our legal and regulatory system with its attitude of knowing ‘no boundaries’.

---

<sup>661</sup> PATRIOT Act, (*Encyclopedia Britannica*) ,available at <https://www.britannica.com/topic/USA-PATRIOT-Act> (Last Visited on January 21, 2020).

### 5.5.1. The Constitution of India

Right to privacy and data protection are not synonymous but holds equal importance and are co-related. The constitution of India contains the provisions of deities also however, rights are always preferred over duties.<sup>662</sup> Right to privacy has found its place under article 21<sup>663</sup> of the Constitution after innumerable attempts which can be seen in numerous cases.<sup>664</sup>

A number of cases are discussed in previous chapters,<sup>665</sup> which acts as a historical guide to the evolution of privacy as a right in India. However a deeper insight of the latest landmark judgment on privacy and data in *K.S. Puttaswamy and Another versus Union of India and Others*<sup>666</sup> seems very important to understand the entire gamut of Aadhar, privacy and data in toto. For this very reason the facts of the entire case has been put in nutshell in the following words:

It is undisputable today that right to privacy is an inherent right and is the soul of every human being. But it may be recalled that recognition of “privacy” as a fundamental right was not easy and have seen numerous Supreme Court verdicts acting derogatory to the verdict of *K.S. Puttaswamy case*. It almost took a decade to say privacy a fundamental right preserved as right to life and personal liberty under article 21 of the Indian Constitution. A constitutional Bench Judgment (9 Bench) in

---

<sup>662</sup> Mr. Jayanta Ghosh & Dr. Uday Shankar, *Privacy and Data Protection Laws in India: A right based Analysis*, 54 (Bharati Law Review, Oct-Dec, 2016).

<sup>663</sup> *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1

<sup>664</sup> *M.P. Sharma v. Satish Chandra*, AIR 1954 SCR 1077, *Kharak Singh v. State*, AIR 1963 SC 1295, *Govind v. State of Madhya Pradesh*, AIR 1975 SC 1378, *R. Rajagopal v. State of Tamil Nadu*, (1994) 6 SCC 632, *Maneka Gandhi v. Union of India* (1978) 1 SCC 248

<sup>665</sup> *Supra* at chapter 2

<sup>666</sup> (2017) 10 SCC 1



this case have undertaken different facets of privacy into consideration. The contents of this case include;-

- (i) Right to privacy as basic core fundamental right;
- (ii) Nature and facets of right to privacy;
- (iii) Restrictions that may be placed on right to privacy;
- (iv) Nature and facets of dignity;
- (v) Article 21 and restrictions that may be placed thereon as per “procedure established by law” ;
- (vi) Preamble, Fundamental rights and Judicial Review and
- (vii) Constitutional Interpretation.

Today privacy forms an intrinsic part of Art. 21. This right is covered under Part III of the Constitution. Articles forming part and parcel of this right comprises of Arts- 21, 19, 14, 25 and 28. The Supreme Court in a number of cases<sup>667</sup> didn't recognize ‘right to privacy’. Two of the prominent judgment includes judgments in *M.P. Sharma*<sup>668</sup> and *Kharak Singh*<sup>669</sup>. Apart from the above mentioned judgments there are other cases where the Supreme Court has decided privacy to be one of the fundamental rights.<sup>670</sup>

The cause of action which arose in this *Puttaswamy case* is the constitutional challenge to the Aadhar Card scheme of Union Government. Collection of biometric data under this scheme was questioned and regarded it as violative of right to privacy.

The question before the Constitutional Bench (9 Bench) in this case to decide were;-

---

<sup>667</sup>*A.K. Gopalan*, AIR 1950 SC 27, *Rustom Cavasjee Cooper*, (1970) 1 SCC 248, *Maneka Gandhi*, (1978) 1 SCC 248

<sup>668</sup> AIR 1954 SC 300

<sup>669</sup> AIR 1963 SC 1295

<sup>670</sup>*Gobind*, (1975) 2 SCC 148, *R. Rajagopal*, (1994) 6 SCC 632, *PUCL*, (1997) 1 SCC 301

- (i) Whether there is any fundamental right to privacy under the constitution and if so, where is it located and what are its contours?
- (ii) What is the ratio decidendi of *M.P. Sharma* and *Kharak Singh* cases and whether those cases are rightly decided?

While entertaining the above two crucial questions, *Per curiam*, it was held that right to “privacy is an intrinsic part of Article 21” and overruled the decision in *M.P. Sharma* and *Kharak Singh*.

Right to privacy is said to have two contents i.e. positive and negative. This right is recognised in Human Rights Act, 1993 too. Even though there is no precise definition of the term Privacy, this right cannot be disregarded as fundamental right. Right to privacy includes personal choice, freedom of expression and right of the individual not to be judged by others. Privacy cannot be lost simply because an individual is in a public place. Privacy attaches to the person.<sup>671</sup>

After the perusal of the judgment of this case, it is apparent that right to privacy is a fundamental right and forms an intrinsic part of human life. This right cannot be taken away from an individual as it is inherent and inalienable right. Right to privacy is well attached to right to dignity. Apart from the constitution this right is recognized in international documents too. This right is the desire of an individual to keep their private life free from intrusion from third party. Privacy is the dignity one like to keep

---

<sup>671</sup> (2017) 10 Supreme Court Cases 1: 2017 SCC OnLine SC 996, available at <https://www.sconline.com/Members/NoteView.aspx?citation=JTXT-0002748027&&&&40&&&&Search&&&&fullscreen&&&&false&&&&> (2017) %2010%20SCC%201&&&&Phrase&&&&FindByCitation&&&&false (last visited on November 28, 2019).

secure, free from interference. This desire of seclusion has to be protected by the Government.

With the momentum of internet in human lives in e-Commerce, this inalienable and inherent right is in great danger. The legal and techno-legal issues coupled with regulatory one are the question of the moment which demands efficient and meticulous solution.

### **5.5.2. The Right to Information Act, 2005**

Right to Information is a constitutional recognized right in India i.e. a fundamental right.<sup>672</sup> ‘Right to information’ has been defined under section 2(j) of this Act.<sup>673</sup> The concerning issues here is that of ‘data’. Whether data kept in public authority are safe or not is the question. The right of an individual to protect its data has been discussed in number of cases. Some of them includes, *Bannett Coleman v. Union of India*<sup>674</sup>, *Indian Express Newspaper (Bombay) v. Union of India*<sup>675</sup> and *PUCL v. Union of India*.<sup>676</sup> In all of these three cases the Court held that, people have the right to express their views, a people have the right to know and people have the right to information. Article 19 of the Indian Constitution has granted right to information to the people as this right is inherent in human lives.<sup>677</sup>

---

<sup>672</sup>The Constitution of India, art. 19 (1) (a)

<sup>673</sup> This Right includes, right to (i) inspection of work, documents, records; (ii) taking notes, extracts or certified copies of documents or records; (iii) taking certified samples of material; (iv) obtaining information in the form of diskettes, floppies, tapes, video cassettes or in any other electronic mode.

<sup>674</sup> AIR 1973 SC 60

<sup>675</sup> (1985)1 SCC 641

<sup>676</sup> (2004) 2 SCC 476

<sup>677</sup> Mr. Jayanta Ghosh and Dr. Uday Shankar, *Privacy and Data Protection Laws in India: A Right Based Analysis*, 64 (Bharati Law Review, Oct-Dec, 2016).

### 5.5.3. The Information Technology Act, 2008

Information Technology Act, of 2008 is the new avatar of Information Technology Act, of 2011. This Act is an extension of the parent Act and aims at the protection of the cyber related issues. While talking about privacy and data protection, two sections of this Act is of great significance i.e. Section 43 A<sup>678</sup> and 72 A.<sup>679</sup> With the growing cyber crimes, the parent Act of 2011 fail short of its curing and preventive measures. As a result several amendments were brought. The final amendment is that of 2008. The Information Technology (Amended) Act, of 2008 was seen as a march towards addressing the multifaceted cyber crimes, but looking at the present scenario, the Act lacks in many ways to address cyber and e-Commerce related crimes.<sup>680</sup>

### 5.5.4. The Personal Data (protection) Bill 2013

At the time of drafting this Bill, it was hoped by the framers that, it shall be applicable to every Indian States. Clause (e) of the definition part of section 2 has defined the

---

<sup>678</sup>Section 43-A.- Compensation for failure to protect data.- Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation, not exceeding five crore rupees, to the person so affected. (Change vide ITAA 2008) Explanation: For the purposes of this section.-

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

<sup>679</sup>Section 72- A .- Punishment for Disclosure of information in breach of lawful contract.- Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person shall be punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both

<sup>680</sup>*Supra* Note 38.

term “biometric data”.<sup>681</sup> Other important terms like “data Subject”<sup>682</sup>, “personal data”<sup>683</sup> and “sensitive personal data”<sup>684</sup> has been defined under clause (ic), (p) and (x) of S. 2 of Personal Data (Protection) Act, 2013, respectively.

### **5.5.5. Intellectual Property Rights (I.P.R.s)**

It is overwhelming to know that data and privacy as a right has also found its place as one of the essential human property which needs protection like other Intellectual properties. To name there exists four types of I.P.R.s in the world which includes, patents, trademarks, copyrights and trade secrets. Among these four, I have discussed Copyright Act of 1957 to understand the status of data in a more precise form.

Data Protection and Intellectual Property law aims at protecting databases. Section 63 B of Indian Copyright Act reads as.-

*“Any person who knowingly makes use on a computer of an infringing copy of computer program shall be liable for infringement”.*<sup>685</sup>

Three factors determine the intellectual property of an individual, they are: labour, skill and judgment factors.<sup>686</sup>

---

<sup>681</sup>Section 2(e). “biometric data”.- means any data relating to the physical, physiological or behavioural characteristics of a person which allow their unique identification including, but not restricted to, facial images, finger prints, hand prints, foot prints, iris recognition, hand writing, typing dynamics, gait analysis and speech recognition.

<sup>682</sup> Section 2(ic)

<sup>683</sup> Section 2 (p)

<sup>684</sup> Section 2(x)

<sup>685</sup>*Supra* Note 38.

<sup>686</sup>*Id.*

The right of the owner of any literary, dramatic, musical, artistic and cinematographic works is recognized by law and the protection of the same is vital. Data protection and database protection *prima facie* appears synonymous but they are not and their protection under copyright Act is really difficult.<sup>687</sup> Data protection refers to protection of informational privacy of individuals, while database protection refers to protection of creativity.

### **5.6. Comparison between Countries**

In the age of internet and technology our data are travelling from one jurisdiction to another without any universally accepted laws to regulate these online transactions. The issue of privacy and data protection is common in almost every corner of the world. Examples can be drawn from the United Kingdom, European Union, United States and India. Each of these countries had enacted laws keeping in view the nature of the crimes in their respective country, however, the birth of technology and internet failed these laws as new threat were born out of it. Among these four countries similarity can be seen between U.K. and E.U., at the one hand and United Nation and India on the other. U.K. is a part of the European Union and has framed all of its laws on the principle laws of European Union, for instance, U.K.'s Data Protection Act of 2018 is a replica of the E.U.'s GDPR. On the other hand both U.S. and India have scattered laws to regulate the privacy and data of its citizens.

It can be said without doubt that U.K. and E.U.'s laws on data and privacy are more promising and effective in this technologically driven era. United States on the other hand is far way better if comparison is to be made with India, because even though,

---

<sup>687</sup>The Copyright (Amendment) Act, 2012, *available at* [https://www.researchgate.net/publication/291354980\\_Copyright\\_Amendment\\_Act\\_A\\_Revisit](https://www.researchgate.net/publication/291354980_Copyright_Amendment_Act_A_Revisit) (last visited on November 28, 2019).

U.S. have scattered laws as that of India, its laws are way better and technologically sound. Coming to India, time and again it has been pointed out that our laws are not efficient to address the issues discussed above. An amendment is sought in the existing laws and a new comprehensive law is very much needed to address these issues at the earliest. India has to frame regulations as that of the EU and U.K. to be efficient in safeguarding the personal data of the customers in e-Commerce.

### **5.7. Conclusion**

The issue of privacy and data protection has emerged to be the two of the most important issues in human technological history. The issues of choice of law and jurisdiction have tagged along with the former two issues making things even more complicated. After the perusal of U.K.'s laws and USA's laws it appears that Indian laws are far behind the race.

Privacy is something personal which holds different values in different individuals. The only thread connecting these different values is everyone's desire to seclude from interference from other fellow human beings. This right is inherent in nature and has to be protected not only in physical world but also in virtual one. Right to privacy and freedom of expression (Article 19) is regarded as part and parcel and are often read together.

Right to privacy is also recognised in international documents. They include, Universal Declaration of Human Rights, International Convention of Civil and Political Rights and Convention on the Rights of the Child (Article 12). In India, right

to privacy is recognised as fundamental rights under article 21 and 19.<sup>688</sup> Every human desires to have a private life and exercise control over their personal information. There should not be any undesirable interference to personal space of any individual; it even includes unjustified surveillance by the State.<sup>689</sup> There is no single uniform definition of the term privacy and data privacy. The lack of comprehensive laws to determine and protect privacy and data of an individual is one of the legal issues in India. Technology no doubt has eased the lives of human beings but time and again it is interfering with the one's personal space in every possible way. Information of individual's is disclosed in two ways. First one is voluntary and second is involuntary.<sup>690</sup> With the growing borderless internet, privacy and data protection of individual's has become topic of debate across the countries.

As discussed above it is a settled position that there are no comprehensive laws in India to deal with the issues of privacy and data protection in e-Commerce. After a comparative study of U.K. E.U. and U.S.A. law, it appears that these three countries has a more promising and solid laws to combat the issues of privacy and data protection of its citizens, unlike India. Issues of choice of law and jurisdiction are also handled meticulously by the Government of these countries. Coming to the U.S.A, there is no single comprehensive law to address the above mentioned issues but there are laws which cover these issues in different sections captioned under different laws. Therefore it can be concluded on the note that even though there is no comprehensive U.S. laws to deal with privacy and data protection of its citizens but these rights are well taken care of by different sets of laws.

---

<sup>688</sup>*Kharak Singh v The State of U.P. and Ors.*, AIR 1963 SC 1295, *Justice K.S. Puttaswamy (Retd.) v Union of India*, (2017) 10 SCC 1.

<sup>689</sup>*Supra* Note 30.

<sup>690</sup>*Id.*



Lastly, coming back to India, it appears very clearly that there is no comprehensive laws to take in hand the issue of privacy and data protection and despite of having statues in the forms of I.P.C., C.P.C, I.T. Act, 2008, Copyright Law and Indian Constitution to name some, these issues are not addressed properly and needs an immediate and effective initiative on the part of the Indian Government

## CHAPTER SIX

### CONCLUSION AND SUGGESTIONS

In a digital global epoch growth of e-Commerce has been fastened by the internet enormously. Transfer of personal data both indoor and abroad has increased at an extreme level. This growth has been made possible only with the internet. The internet has shaped the art of modern technology. Even in the traditional society, people were engaged in commerce but today the commerce in which our society is actively involved is in e-Commerce. The difference which can be drawn between the two is, in the former one, business involved people coming together physically. For instance, the earlier human practiced barter system (exchange of goods with goods, which involved physical presence of the both), later the most advanced form of traditional commerce was between the bank and the people (where people physically went to the bank for saving and other cash related transactions). Then later on, with the fast growing internet, society indulged in the digital form of commerce popularly known as the 'e-Commerce'. The way business is conducted today has changed drastically as it used to be conducted before. While addressing the growth of commerce, some scholars have even made reference to the Roman Empires which is considered to have brought trade and commerce in Europe.

The most accepted definition of the term 'commerce' is buying and selling of goods and services. One has to dig into the history of information technology to understand the journey of e-Commerce. The technology has evolved the way commerce is

performed today and has switched the physical involvement of people with the virtual fashion of e-Commerce. Now anyone anywhere can engage in buying and selling of goods and services. The buyers and sellers do not come face to face as everything is possible online 24 x 7. The credit for the evolution of e-Commerce owes to the introduction of Information and Communication Technology (ICT) and World Wide Web (WWW). The well-known types of e-Commerce are of four types i.e. B2C, B2B, C2C and C2B. This new forms of commerce are time and cost effective. Every form of buying and selling happens online. It does not require the concerned parties to come face to face. The most interesting thing about e-Commerce is people can do business from anywhere and anytime and consumers can avail information about the desired products with the help of web pages. E mail is another medium which facilitates the buyer to avail the services. Having regards to the perks internet and the technology has provided to the human society, the loopholes it holds cannot be denied by the advocates of privacy and data protection. Scholar's looks at internet as an insecure medium and Yes, they are right, it is an insecure medium because we do not know with whom we are doing business and the numbers of people involved are behind the veil. There are intermediaries commonly known as the middle men in internet who facilitates the services but their liability in occasions of legal and techno-legal issues are limited. Therefore, who will be liable in the events when intermediaries are within the exception of the law?

The Indian society is not actively engaged and aware about their privacy and data protection rights as much as that of the European Union and U.K. Citizens. Not only are the citizens of these two countries are conscious but the Government too is more vibrant and result oriented in the domain of privacy and data protection. The lack of

knowledge among the Indian consumers along with the absence of sensitization programs attributes to the issues of privacy and data protection coupled with other legal, techno-legal and regulatory issues. The legally handicapped privacy and data protection laws in the one hand and the unaware consumers on the other have seriously necessitated for having a comprehensive privacy and data protection law in India.

Privacy is the conscious as well as unconscious demand of an individual. Though this right is well accepted to be inherent human rights, protecting one is not easy. The lack of uniform definition makes it difficult to claim this right. The concept of privacy varies from one individual to another and that between different countries. The dawn of technology has intruded the privacy and data protection of people. It is natural for every person to set boundaries and claim privacy against intrusion from other human beings and in some case from the Government too.

There cannot be one correct definition of the term 'privacy'. There are different contours of privacy. The advancement in technology and online platform beyond one's control and unlimited nature of jurisdiction made a gateway to unstoppable cyber crimes which are difficult to curb down in the absence of effective laws. Though a new beam of hope is drawn by the Data Protection Bill and Consumer Protection Bill, 2018, our people as well as legal and regulatory authorities are still praying to see the actual light. Our laws have proven again and again to be inefficient in front of the giant technology which is targeting consumer's data and privacy at an alarming speed. Consumers are victims of technological advancement and online transactions which takes place at anytime and anywhere. In the absence of laws on

privacy and data, it becomes very difficult to safeguard one's privacy and data. The problem is more severe when data is transferred from one jurisdiction to another without obtaining prior permission or knowledge of the data subjects.

The legal issues arising in respect of the use of computers or the internet are not addressed and the laws in hand are also inefficient to decide on these matters. The other tricky legal issue is that of protection of personal data. The person in hold of such data may even loose his right over the same, if he is not careful during online activities. In the growing trend of electronic commerce, India does not have proper law to address the privacy and data related issues .Wider use of internet for multiple purposes, implicates data of those going online and personal data coming into India through transborder flow does not have any protection here at all. India needs guidelines on transborder flows of personal data as that of the OECD (Transborder Flows of Personal Data 1980) to keep track of every data that comes and goes. Internet world calls for India to now have legislation on the protection of privacy and Data protection on an online world.

Privacy is something personal which holds different values in every individual. The only thread similar among every individual is their desire to seclude from interference from other fellow human beings. This right is inherent in nature and has to be protected not only in physical world but also in virtual one. Right to privacy and freedom of expression (Article 19) is regarded as part and parcel and are often read together.

The objective of this research work was mainly divided under the three areas. The first one was to study the issues, arising in respect of privacy and data protection in e-Commerce in India and to critically identify the deficiencies in the current framework of e-Commerce Regulations in India and investigate requisite amendments. This objective have been tried to achieve in chapter one and three of the thesis. After doing a literature review of various authors on the issues of privacy and data protection, it is found that these issues mainly started with the development of internet. Prior to the growth of internet and technology there were no such issues as they were closely guarded and limited to access by other human beings. As change is continuous in human lives, the concept of privacy and data protection gradually evolved over the years. The issue of privacy and data protection is the result of borderless internet.

Second objective was to analyse the grey areas on imposition of the liability on the intermediaries in matters relating to issues concerning privacy and data protection in e-Commerce- in India as well as in cross- border e-Commerce. The Information Technology Act, 2000, only provides punishment for violation of privacy, without even defining the term. The Act is vague in matters of protection of privacy and data privacy and there is a no due care liability of the service provider for the data protection in India.

Third objective was to study and analyze the problems of tracking activities done by cookies, data mining and issues of security and uninterrupted login in e-commerce faced by e-consumers and their prospective solutions, this last objective have been addressed in chapter two of the thesis under the sub-heading techno-legal issues. There is no law to effectively address these issues in India. Privacy and data of

consumers are not safe in internet jurisdiction as there is no court to hear the matter. There are no consent principles in social networking sites including social messaging sites like Facebook, which provide the liberty to the user's to deny information's which they think are personal nor the Indian Government has come up with strict policies to restrict these social networking sites that holds records and sensitive information's. The issue of security over internet is very crucial in India, as there are no comprehensive laws to check security of the data and privacy of an individual which travels to third parties without prior consent or knowledge of the data subject for commercialization. Data mining is another critical issue as huge data travels from one jurisdiction to another or multiple jurisdictions with no identification of the person, single law or court to address the matters in times of violation of the data subject's rights.

The hypothesis of the thesis were, (i) existing laws in e-Commerce are not adequate to address the legal and techno-legal issues of Privacy and Data Protection and (ii) there is a no due care liability of the service provider for the data protection. After a careful reading of the Indian statutes and analyzing the issues of privacy and data protection in e-Commerce, it is evident that the existing laws in e-Commerce are not adequate to address the legal and techno-legal issues of Privacy and Data Protection and there is a no due care liability of the service provider for the data protection. Hence, both of the hypotheses are proved.

### **Suggestions:**

After the thorough perusal and sincere effort to understand the available researched works on the issue of privacy and data especially in the e-Commerce, it appears to be

politically correct to give a statement that India is legally handicapped and has kneeled down before the giant technology. The aged old laws along with the contemporary ones which was specifically designed to address the e-Commerce related issues miserably fails to keep a amicable tandem with the mushrooming menace of technology. The valuable suggestions is expected to serve as a guiding torch for the legislatures for understanding the prevailing situations and the enormous harms done by the internet to our privacy, personal space and sensitive personal data's on day to day basis.

Following are some of the suggestions which I feel are needed at this hour of the calamities done to our privacy and data.

- 1. Amendments in the Information Technology Act, 2008:** Information technology Act, 2000 came with the purpose to legalize e-contracts and digital signatures along with the intention to flourish e-Commerce laws for India. Having failed to serve its ends in several areas this Act was amended several times, the latest is that of 2008. The legislators have failed to realize the importance of incorporating a legal definition of the term **privacy** and **data privacy** in the Act.

It has been a debate for many decades on the topic that, '*there is no uniform definition of the term privacy*' and internet is encroaching in the private space of the people and mis-using their data without their knowledge and consent. In such circumstances absence of any laws which defines these two terms would be like voluntary turning into deaf and dumb.



In my opinion there must be an amendment in the present Information Technology Act, and should incorporate these two terms i.e. privacy and data privacy and should also define as to what constitutes sensitive personal data.

OR

- 2. A comprehensive privacy and data Law:** India does have this Information Technology Act, 2008, Indian Penal Code, 1806, Indian Evidence Act, Indian Contract Act, Code of Civil Procedure, Consumer Protection Act, SEBI and R.B.I. guidelines too but these Acts and guidelines even if read together or codified as one will not be able to address the issues of privacy and data protection in e-Commerce. The issues of privacy and data in India are the result of scattered laws. The traditional laws are not efficient enough to tackle these two issues in e-Commerce platform because of the simple reason that internet is dynamic and these Acts are static. These two problems are even more severe when transactions in e-Commerce involve parties of different jurisdictions. Internet knows no boundaries whereas, consumers and courts of any country are bounded by the principles of jurisdiction. In such circumstances the issue is that of choice of law, choice of forum and choice of jurisdiction. Which laws shall be binding on the parties involved and whether the verdict of the courts will be binding on them is the other questions that's need to be addressed as soon as possible. This problem will continue if the legislatures do not legislate a privacy and data law which would define privacy, data privacy and be comprehensive enough to address the issues involved in e-Commerce transactions.

**3. A Uniform Cyber Law for e-Commerce:** E-Commerce is totally dependent on the internet services and due to the fact that internet is borderless and involves parties across the world, there is a serious requirement to have a uniform cyber law to address the issues of privacy and data protection of every parties involved in e-commerce transactions. Every country involved in this business must come together and formulate a uniform law to serve the purpose of addressing the issues arising between people of different jurisdictions without prejudicing the laws of their lands. The law of one country does differ from the another owing to the practices and prevailing situations and demands but as internet is borderless and involves parties of different jurisdictions governed by their own laws it is impossible to apply the law of only one country, hence, if there is a uniform cyber law on e-Commerce it will be easy to address the conflict.

**4. Defining the term ‘e-Commerce’ & ‘e-Consumers’:** In India we have consumer related Acts, in the form of Consumer Protection Act, 1986 and Consumer Protection Act, 2019. None of the above Acts defines the term ‘e-Commerce’ & ‘e-Consumers’. Therefore, I would suggest amendment in the former Act, to insert these terms for better understanding and clarity.

**5. Amendment in the Information Technology (Intermediaries Guidelines) Rules, 2011:** Internet world involves active participation of intermediaries. The role of these middlemen is very important in e-Commerce. There are guidelines on Intermediaries in India but not good enough to handle the cross-border issues of privacy and data protection in e-Commerce. As per these guidelines, the intermediaries shall not be liable if they prove that they were

not negligent during the course of their work. In such circumstances, the consumers are the only one who will suffer the damage. The government should make such guidelines on Intermediaries which would be comprehensive enough to address the core issues involving consumers in e-Commerce transactions within as well as across the country.

- 6. Laws on transborder flow of data:** Data travels from one jurisdiction to another in the shortest time with the help of internet. Such data may contain data which are personal and sensitive in nature like health details, accounts details, personal preference etc. In the absence of law to check the flows of data from one jurisdiction to another, it would create confusion and will lose track of those data. At this internet age it is very common to share personal details for availing of online services and people might get denied of that service in failure of non-disclosure of certain personal details. There should be a 'consent option' in every services facilitated by the online platform along with the short information regarding safety undertakings by those service providers regarding the safety of those data.
- 7. Separate Online privacy law for children:** The Indian Government must take initiative to frame a separate Online Privacy Law for children who are engaged in web sites and personal messaging social networks like Facebook. The Act must aim to control the transfer of their personal information, like the U.S. COPPA Act, 1998.
- 8. E-Commerce Dispute Resolution Forum:** The speed at which e-Commerce is trending in India, there is a need to strengthen the e-CommerceDispute

Resolution. Formation of such kind of forum shall help the consumers to put forward their grievance at the earliest possible time.

**9. Application of the theory of ‘*Lex loci delicti*’ in internet :** In occasions of any form of disputes in e-Commerce the theory of ‘*Lex loci delicti*’ should be applied to resolve the issues at the earliest and without confusion of law and jurisdiction . The Country where the wrong have been committed should be the country to act upon the matter before its court irrespective of the jurisdictions of the parties involved.

**10. Easy Privacy Clauses and specific purchasing rules:** Privacy Clauses in India are either complicated or compulsory which compels the customers and people in toto to reluctantly adhere to the privacy norms posed by companies in exchange of the service demanded. Is it legally sound to force the people to give their consent? Is it not violative of their fundamental right or such act arbitrary in the eye of law? Many would agree that yes it is unlawful and violative of the constitutional rights. Here I would like to draw the attention on the European Union’s GDPR (General Data Protection Act) 2018. This Act is a modernize law for the protection of personal information of the customers of European Union. It also came to harmonise data protection laws across Europe. At this juncture I would like to appeal our legislature to give a thought on having customer oriented laws for their privacy and data protection. The cyber world threatens our personal information at each stage of life. Without strong privacy Clause no consumer will escape from cyber exploitation. Consumers must be given protection under our law and standard purchasing

rules must also be provided so that their consent will be optional rather than a mandatory one. Consent of the customers should be of utmost importance.

#### **11. Conducting Compulsory awareness programme to the entire Cyber Café**

**Owner:** Taking into consideration the growing menace of computer related crimes, I would suggest conducting compulsory awareness programme to all the owners of cyber hub regarding crimes which are conducted through use of computer and internet. I would also appeal them to approach the Police official to set up a committee where they can work in coordination to target the cyber-criminals. Keeping a bird eye view on the customers is highly demanded.

#### **12. Sensitization Programmes at Schools, Rural areas as well as in Urban**

**areas:** Intrusion into one's private space and misuse of personal data are the two most crucial issues in e-Commerce today. Internet and technology together has formed an integral part of human lives. The lives of the people of all age groups have been touched by this technology. All the strata of a society are making the most of the facilities offered by the internet without realizing the damages it has been doing to our privacy and data. People have so much so surrendered themselves to the easy lifestyles provided by these technology that unknowingly they have invited the darker side of the internet.

With the introduction of social platforms like Facebook and WhatsApp, cyber related crimes have increased numerous over the years and the mostly targeted groups are the students and youths. The lack of knowledge about

cybercrimes is another issue which demands attention of the government as well as attention of the parents. The sensitization programme at schools regarding the cyber related crimes, privacy and data is really important at this internet age. Such sensitization programme should also involve the active participation of both the parents as parents should also know and understand these issues and they would be the best people to teach their children's all over again at home in a friendly environment regarding the pros and cons of social networking sites.

In the rural and urban areas people of all age groups are engaged in an online shopping. Social networking sites like Facebook and e-Mails are also common. Due to the lack of knowledge as well as awareness on privacy and data protection issues, people have felled and are still falling prey to the menace offered by this technological involvement in our lives. Online shopping is one of the best examples of e-Commerce which is facilitated by the internet. Without obtaining the consent of the consumers these online shopping sites are using the personal information of these people for commercial gains. The saddest part is most of the people do not know and even don't care even if their personal information's and data are misused by third parties. In addition there are issues like profiling of pictures in Facebook. Due to the lack of security in these social networking sites, any one from anywhere can create a fake account, put up profile picture of another person and dupe people for immoral gains. How to identify these fake people and stop making of fake profiles are another milestones. The best thing to do initially is to arrange a sensitization programme in the areas mentioned above on the

topics like Cyber Crimes, Cyber laws, on importance on privacy and data protection, Redressal forum in occasions of any issues discussed above and other important issues which is necessary to converse about.

## REFERENCES

1. Abhinav Gupta, *Privacy: Whether a Fundamental Right?* 3 (Foreword by Prof. Dr. S. Rajendra Babu), “A Public Discourse on Privacy-An Analysis of Justice K.S. Puttaswami v Union of India” (Dr. R. Venkata Rao & Dr. T.V. Subba Rao Edtrs.).
  2. A. Kranthi Kumar Reddy, et.al, *Cyber Space and the Law-Issues and Challenges* 202 (Published by, NALSAR University) (Printed at, the Print House, Hyderabad) (2004).
  3. Aadhar system, Available at <https://timesofindia.indiatimes.com/india/hackers-deposit-re-1-in-trai-chiefs-account/articleshow/65190556.cms> (Last visited on July 31, 2018).
  4. “Aadhar”, Available at <https://www.indiatimes.com/technology/news/after-aadhaar-leak-hacker-deposits-rs-1-in-trai-chairman-s-account-to-improve-system-s-privacy-350316.html> (Last visited on July 31, 2018).
  5. A. Mohamed Mustaque “Online Dispute Resolution with Special Emphasis on Mediation in India” (2012) 4 SCC J-7, available at <https://www.sconline.com/Members/SearchResult.aspx> (Last visited on September 9, 2019).
  6. Agrima Srivastava, *Enhancing Privacy in Online Social Networks using Data Analysis* (2015), (Unpublished Ph.D. thesis, Birla Institute of Technology, Pilani)
  7. Alwyn Didar Singh *E-Commerce In India: Assessment and Strategies for the Developing World* 778-782 (2008) (LexisNexis, Butterworths Publication).
  8. Amarnath Mitra, “RFID in India: Implementation, Issues and Challenges”, available at <https://imanagerpublications.com/index.php/article/2942> (Last visited on August 20, 2018).
  9. Anmol Kumar, Privacy and Sensitive Information, Available at [https://shodhganga.inflibnet.ac.in/bitstream/10603/132472/10/10\\_chapter%205.pdf](https://shodhganga.inflibnet.ac.in/bitstream/10603/132472/10/10_chapter%205.pdf)
-



- f (Last visited on January 15, 2019)., Amit Kumar Tyagi, *et.al*,(Volume 4, Special Issue 1, February 2014), *available at*[http://www.ijetae.com/files/ICADET14/IJETAE\\_ICADET\\_14\\_01.pdf](http://www.ijetae.com/files/ICADET14/IJETAE_ICADET_14_01.pdf) (Last visited on June 27, 2017).
10. Aparna Viswanatha, *Cyber Law, Indian & International Perspectives*, 31 (Published by LexisNexis Butterworths Wadhwa Nagpur).
  11. Aravind Menon *THE eLAWS* 359 (Forwarded by Hon'ble Mr. Justice K.T. Thomas) (1<sup>st</sup> Edn. 2011).
  12. Article 19, guaranteeing a certain freedom was held exclusionary from Article 21, guaranteeing life and personal liberty, *available at* <https://www.livemint.com/Politics/7oHGx6UJfLD0uIDXFwV9CL/Is-privacy-a-fundamental-right-Two-cases-that-Supreme-Court.html> (Last visited on December 19, 2018).
  13. Arun Mal & Jenisha Parikh, "Facebook and Right to Privacy: Walking a Tight Rope" (2011) 4 *NUJS L Rev* 299, *available at* <https://www.scconline.com/Members/NoteView2014.aspx?citation=JTXT-0000003719&&&&40&&&&Search&&&&fullscreen> (Last visited on October 19, 2018).
  14. A. Sengupta et al, e-Commerce security- A life cycle approach , (Vol.30, parts 2 & 3, April/June 2005, p. 119-140), *available at* <http://www.ias.ac.in/article/fulltext/sadh/030/02-03/0119-0140> (Last visited on June 22, 2017).
  15. Asia-Pacific Economic Cooperation, *available at* [https://en.wikipedia.org/wiki/Asia-Pacific\\_Economic\\_Cooperation](https://en.wikipedia.org/wiki/Asia-Pacific_Economic_Cooperation) (Last visited on March 23, 2019).
  16. Barkha and U. Rama Mohan, *Cyber Law & Crimes* 165 (Published by S.P. GOGIA, H.U.F.) (2013).
  17. Benjamin Wilson, *Data Privacy in India: The Information Technology Act*, (Posted on February 8, 2019), *available at*
-

- [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3323479](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3323479) (Last visited on January 27, 2020).
18. Blog, Available at <https://en.wikipedia.org/wiki/Blog> (Last visited on July 23, 2018).
  19. BP Dwivedi “Emerging Right to Privacy an Indian Perspective” “Conceptual and Constitutional Foundation”, *available at* [http://shodhganga.inflibnet.ac.in/bitstream/10603/137097/7/07\\_chapter\\_02.pdf](http://shodhganga.inflibnet.ac.in/bitstream/10603/137097/7/07_chapter_02.pdf) (Last visited on September 4, 2018).
  20. Browser, Available at <https://searchwindevelopment.techtarget.com/definition/browser> (Last visited on July 23, 2018).
  21. Children’s Online Privacy Protection Act, 1998, *available at* <https://www.inc.com/encyclopedia/childrens-online-privacy-protection-act-coppa.html> (Last visited January 22, 2020).
  22. Choice of Law, *available at* [https://en.wikipedia.org/wiki/Choice\\_of\\_law](https://en.wikipedia.org/wiki/Choice_of_law) (last visited on November 28, 2019).
  23. Chris Reed, *Internet Law* 262-263 (Universal Law Publishing, Co. Pvt. Ltd) (2<sup>nd</sup> Edn.) (2010).
  24. Cloud Computing, Available at *available at* <https://azure.microsoft.com/en-in/overview/what-is-cloud-computing/> (Last visited on July 23, 2018).
  25. Cloud Service Providers, Available at <https://www.techopedia.com/definition/18977/data-processor> (Last visited on 23-07-2018).
  26. Computer Virus, available at [https://en.wikipedia.org/wiki/Computer\\_virus](https://en.wikipedia.org/wiki/Computer_virus) (Last visited on July 23, 2018).
  27. Computer Crimes, Available at [https://en.wikipedia.org/wiki/Surface\\_computer](https://en.wikipedia.org/wiki/Surface_computer) (Last visited on December 21, 2018).
  28. Computer Matching and Privacy Act, 1988, *available at* [https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/inforeg/inforeg/final\\_guidance\\_pl100-503.pdf](https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/inforeg/inforeg/final_guidance_pl100-503.pdf) (Last visited on January 21, 2020).
-

29. The Copyright (Amendment) Act, 2012, *available at* [https://www.researchgate.net/publication/291354980\\_Copyright\\_Amendment\\_Act\\_A\\_Revisit](https://www.researchgate.net/publication/291354980_Copyright_Amendment_Act_A_Revisit) (last visited on November 28, 2019).
  30. Conclusion & Suggestion, *available at* [http://shodhganga.inflibnet.ac.in/bitstream/10603/52364/16/16\\_conclusion.pdf](http://shodhganga.inflibnet.ac.in/bitstream/10603/52364/16/16_conclusion.pdf) (Last visited on October 3, 2018).
  31. Code of Civil Procedure, 1908
  32. Constitution of India
  33. Consumer Protection Act, (COPRA)1986
  34. Consumer Protection Act , 2019 (Act 35 of 2019)
  35. Confidential Information, Available [at](https://www.techopedia.com/definition/29060/security-breach) <https://www.techopedia.com/definition/29060/security-breach> (Last visited on July 23, 2018).
  36. Cyber Crime, Available at <https://www.coe.int/en/web/cybercrime/the-budapest-convention> (Last visited on July 23, 2018).
  37. Danielle Keats Citron, *Mainstreaming Privacy Torts* 1807.
  38. Data Privacy, Available at <https://en.wikipedia.org/w/index.php?search=Data+privacy&title=Special:Search&profile=default&fulltext=1&searchToken=7r2p9ktjwll6izasy5225ec86> (Last visited on July 23, 2018).
  39. Data Analytics Controller, Available at *available at* <https://www.sebi.gov.in/pdf/guidelines-of-data-sharing-final.pdf> (Last visited on February 6, 2020).
  40. Data Expunging, Available at <https://www.sebi.gov.in/pdf/guidelines-of-data-sharing-final.pdf> (Last visited on February 6, 2020).
  41. Data Anonymization, Available at <https://www.sebi.gov.in/pdf/guidelines-of-data-sharing-final.pdf> (Last visited on February 6, 2020).
  42. Data Protection Policy-Data Protection Act of 2018, *available at* [http://salisburygroup.com/sites/default/files/2018-09/Data%20Protection%20Policy%20\(Web%20Version\).pdf](http://salisburygroup.com/sites/default/files/2018-09/Data%20Protection%20Policy%20(Web%20Version).pdf) (last visited on November 07, 2019).
  43. Data Seeker, Available at <https://www.sebi.gov.in/pdf/guidelines-of-data-sharing-final.pdf> (Last visited on February 6, 2020).
-

44. David J. Kessler, Sue Ross & Elonnai, “A Comparative Analysis of Indian Privacy Law and the Asia Pacific Economic Cooperation Cross –Border Privacy Rules”, *NLSIU-6* (2014).
  45. Dennis Marks “What is the difference between Cookies and Tracking Tags” (March 22, 2018) *available at* <https://www.quora.com/What-is-the-difference-between-cookies-and-tracking-tags> (Last visited on October, 4, 2018).
  46. Denis Sparas, EU Regulatory Framework for e-commerce, WTO Workshop, Geneva, 18<sup>th</sup> June 2013, *available at* [https://www.wto.org/english/tratop\\_e/serv\\_e/wkshop\\_june13\\_e/sparas\\_e.pdf](https://www.wto.org/english/tratop_e/serv_e/wkshop_june13_e/sparas_e.pdf) (last visited, November 19, 2019).
  47. Desai, Prashant S,” Legal protection of right to privacy in the era of information technology a critique” “Information Technology and Threat to Privacy -An Analysis”, *available at* [http://shodhganga.inflibnet.ac.in/bitstream/10603/98806/13/13\\_chapter%206.pdf](http://shodhganga.inflibnet.ac.in/bitstream/10603/98806/13/13_chapter%206.pdf) (Last visited on August 31, 2018).
  48. Diane Rowland, Uta Kohl, *et. al.*, *Information Technology Law*, 162 (British Library Cataloging in Publication Data, 4<sup>th</sup> Edn.)(2012).
  49. Dileep Kumar Singh & Vishnu Swaroop, “Data Security and Privacy in Data Mining: Research Issues & Preparation” (volume 4, Issue2- 2013), *available at* <http://ijcttjournal.org/Volume4/issue-2/IJCTT-V4I2P129.pdf> (Last visited on June 27, 2017).
  50. Disputes, *available at* <https://cyber.harvard.edu/olds/ecommerce/disputes.html> (last visited on 28 November, 2019).
  51. Dr. Amita Verma, *Cyber Crimes and Law*, 318,323 (Central Law Publications) (2009).
  52. Dr. R. Venkata Rao & Dr. T.V. Subba Rao (eds.) *52 A Public Discourse on Privacy-An Analysis of Justice K.S. Puttaswamy v Union of India* (Foreword by Hon’ble Justice Prof. Dr. S. Rajendra Babu)
  53. Dr. Rakesh Kumar and Ajay Bhupen Jaiswal *Cyber Laws* 95 (APH Publishing Corporation) (2011).
  54. Dr. S.V. Joga Rao, “Law of Cyber Crimes & Information Technology Law” 234-235.
-

55. ECPA, 1986, *available at* <https://www.sciencedirect.com/topics/computer-science/electronic-communications-privacy-act> (Last visited on January 23, 2020).
  56. E.J. Jathin “Human Genome Project: Emerging Challenges of Right to Privacy vis-à-vis Insurer’s Right to Know” 2 (Vol. XXXI) (March-June) *C.U.L.R.* (Number 1&2) (D. Rajeev Edtr.),(N.S. Gopalkrishnan & A.M. Varkey (eds.) (2007).
  57. Emil Sit & Kevin Fu, “*Web Cookies: Not Just a Privacy Risk*”, (September 2001/Vol. 44, No. 9), *available at* <https://courses.cs.washington.edu/courses/cse484/14au/reading/cookies-risk.pdf>, (Last visited on July 4, 2017).
  58. E.N. Murthy *Internet Phishing: Techno-Legal Approach* 5, GRK Murthy & C Sri Krishna (eds.) (Vol. IX), Nos. 1& 2) *ICFAI JL. Of Cyber Law* (February and May 2010) (IUP Publications) (Printed at M/S ICIT Software Centre Pvt. Ltd.,).
  59. EN Murthy and GRK Murthy Eds. “Data Mining: Legal Implications” (Vol. VIII No. 2) (p.5)(May 2009) (Published on behalf of the ICFAI University press, # 52, Nagarjuna Hills, Panjagutta Hyderabad 5000082, Andhra Pradesh) (Printed at M/S. ICIT Software Center Pvt. Ltd., # 1, Andhra Pradesh)
  60. Encryption, Available at <https://en.wikipedia.org/wiki/Encryption> (Last visited on 23, 2018) (at 16:19 PM).
  61. E- Z Pass, Available at [https://en.wikibooks.org/wiki/Transportation\\_Systems\\_Casebook/Tolling/E-ZPass](https://en.wikibooks.org/wiki/Transportation_Systems_Casebook/Tolling/E-ZPass) (Last visited on October 04, 2018).
  62. Ferdinand J. Jr. Zeni “*Wiretapping-The Right of Privacy versus the Public Interest*” (Volume 40) (Issue 4) (Journal of Criminal Law and Criminology)(Article 5) (J. Crim. L. & Criminology 476 (1949-1950), *available at*<https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=3703&context=jcllc> (Last visited on October, 03, 2018).
  63. Forbes, *available at* <https://www.forbes.com/sites/kalevleertaru/2019/03/23/facebook-succeeded-in-killing-cybersecurity-like-it-did-privacy/#52e30db84549> (Last visited on January 16, 2020).
  64. Fraud, Available at <https://en.wikipedia.org/wiki/Fraud> (Last visited on December 18, 2017).
-

65. Gavin Phillipson and Heklen Fenwick “Breach of Confidence as a Privacy Remedy in the Human Rights Act Era” *Modern Law Review* (p. 662) (2000) (Vol.63) (No.1) (Jan-Nov.) (Published for the Modern Law Review limited by publishers).
  66. Geetha Nondikotkur “SEBI Issues Risk Framework Guidelines” (July 8 2015), *available at* <https://www.bankinfosecurity.com/sebi-issues-risk-framework-guidelines-a-8383> (Last visited on August 10, 2018).
  67. Genetic Privacy, Available at <https://en.wikipedia.org/w/index.php?search=Genetic+privacy&title=Special:Search&profile=default&fulltext=1&searchToken=5lecq6ozrmlbw3mg6i103jj1r> (Last visited on July 23, 2018).
  68. G.K. Kapoor, “Defective Goods and Deficiency of Services Vis a Vis Consumer”, *available at* [http://www.consumereducation.in/monograms/7\\_diffective\\_goods\\_and\\_deficiency\\_o\\_services\\_vis\\_A\\_Vis\\_consumer.pdf](http://www.consumereducation.in/monograms/7_diffective_goods_and_deficiency_o_services_vis_A_Vis_consumer.pdf) (Last visited on March 23, 2019).
  69. Grant Kelly and Bruce McKenzie, Security, privacy, and confidentiality issues on the Internet (2002), *available at* <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1761937/> (Last visited on November 18, 17).
  70. Hacking, Available at *available at* [https://en.wikipedia.org/wiki/Email\\_hacking](https://en.wikipedia.org/wiki/Email_hacking) (Last visited on August 10, 2018).
  71. Ian J. Llyod, *Information Technology Law 17* (Published by, Oxford University Press 198 Madison Avenue, New York, United States of America) (Printed in, Ashford Colour Press Ltd, Gosport, Hampshire) (7<sup>th</sup> Edition, 2014).
  72. Identity theft, Available at <https://www.investopedia.com/terms/i/identitytheft.asp> (Last visited on July 23, 2018).
  73. Importance of Right to be ‘left alone’ and ‘Anxiety over privacy’ were also instituted in UK. ‘Anxiety UK’ is another important aspect in UK, which ensures and respect privacy of an individual, *available at* <https://www.anxietyuk.org.uk/privacy-policy/> (Last visited on October 19, 2018).
  74. Indian Penal Code, 1806
  75. Indian Laws dealing with Data Protection, *available at* <http://vikaspedia.in/e-governance/national-e-governance-plan/data-privacy-and-protection/indian-laws-dealing-with-data-protection> (Last visited on August 8, 2018).
-

76. Information Privacy, Available at [https://www.researchgate.net/publication/259502676\\_State\\_of\\_the\\_Information\\_Privacy\\_Literature\\_Where\\_are](https://www.researchgate.net/publication/259502676_State_of_the_Information_Privacy_Literature_Where_are)
77. Internet Protocol, Available at *available at* [http://www.linfo.org/packet\\_header.html](http://www.linfo.org/packet_header.html) (Last visited on February 7, 2020).
78. IP Concerns about International Transaction in E-Commerce, *available at* [https://www.wipo.int/sme/en/e\\_commerce/transactions.htm](https://www.wipo.int/sme/en/e_commerce/transactions.htm) (Last visited on March 26, 2019).
79. Intermediary Liability, Available at <https://blog.chavannes.net/wp-content/uploads/2017/05/Intermediary-liability-IvIR-2017.pdf> (Last visited on December 9, 2019).
80. Issue of confidentiality, *available at* <http://www.legalserviceindia.com/article/1413-Breach-Of-Confidentiality-&-Various-Legal-Issues.html> (Last visited on October 21, 2018).
81. It aims at, Basic rights, Right to be informed and Right to Participate, *available at* <https://www.youtube.com/watch?v=T8rMS2nKMmI> (Last visited on October 6, 2018).
82. James Frew, Security Threats Users Need to Know About, (Updated on December 17, 2019), *available at* <https://www.makeuseof.com/tag/4-security-threats-whatsapp-users-need-know/> (Last visited on January, 16, 2020).
83. Jan Henrik Ziegeldorf, Oscar Garcia Morchon, et.al, *Privacy in the Internet of Thing: Threats and Challenges*, *available at* <https://arxiv.org/ftp/arxiv/papers/1505/1505.07683.pdf> (Last visited on October 04, 2018).
84. Jayanti Ghosh and Uday Shankar “Privacy and Data Protection Laws in India: A Right-Based Analysis” *Bharati Law Review* (65-66) (2016).
85. Jeremy James “Privacy and RFID” (Published in Mar. 25, 2013), *available at* <https://www.youtube.com/watch?v=UMFXce79PD0> (Last visited on October 04, 2018).
86. Joshika Thapa, *Jurisdictional Issues in Cross border e-Commerce Disputes: A Critical Study* (2018) (Unpublished M.Phil. thesis, Sikkim University).
87. Jurisdiction in International Law, Available at <https://arxiv.org/ftp/arxiv/papers/1505/1505.07683.pdf> (Last visited on June 28, 2019).
-

88. Jurisdiction under the Information Technology Act, 2000 *available at* [https://shodhganga.inflibnet.ac.in/bitstream/10603/7829/14/14\\_chapter%205.pdf](https://shodhganga.inflibnet.ac.in/bitstream/10603/7829/14/14_chapter%205.pdf) (Last visited on September 23, 2019)
89. Justice Yatindra Singh, *Cyber Laws* 117 (Universal Law Publishing Co. Pvt. Ltd.) (2008).
90. Kamiel J. Koelman, “Online Intermediary Liability”, *Copyright Electronic Commerce, Legal Aspects of Electronic Copyright Management* 7, (Editor, P. Bernt Hugenholtz), (2000), (Published by , Kluwer Law International Ltd, London, United Kingdom).
91. Karnika Seth, *Computers, Internet and New Technology Laws* 281, A Comprehensive work with a special focus on developments in India, (1<sup>st</sup> Edn.).
92. Kavita, *Copyright in the Digital Age: Internet Issue* (2015), Available at [http://shodhganga.inflibnet.ac.in/bitstream/10603/100920/1/01\\_title.pdf](http://shodhganga.inflibnet.ac.in/bitstream/10603/100920/1/01_title.pdf) (Last visited on October 1, 2018).
93. K. Susheel Barath & Dr. V. Mahalakshmi, “Legal Issues in e-commerce transactions –An Indian Perspective”, 185, (Volume 4, Issue 11,) (International Journal on Recent and Innovation Trends in Computing and Communication), *available at* <https://ijritcc.org/index.php/ijritcc> (Last visited on December 13, 2020).
94. Kuldeep Kaur et al, “E-Commerce Privacy and Security System”, (Vol.5, Issue 5, Part-6) May (p. 63-73), (2015) [http://www.ijera.com/papers/Vol5\\_issue5/Part%20-%206/J505066373.pdf](http://www.ijera.com/papers/Vol5_issue5/Part%20-%206/J505066373.pdf) (Visited on June 20, 2017).
95. Latha R. Nair, “Data Protection efforts in India: Blind Leading the Blind?” 2 (*NLSIU India Journal of Law and Technology*) (Westlaw India) (2008).
96. Laura Hildner “Defusing the Threat of RFID: Protecting Consumer Privacy, Through Technology-Specific Legislation at the State Level” (Eun Young & Jocelyn Simonson et al Edtrs.) (*Harvard CIVIL RIGHTS, CIVIL LIBERTIES LAW REVIEW Vol. 41, Winter 2006*) (1-2 (No. 1)2006) (Publication Centre: Harvard Civil Rights-Civil Liberties Law Review, 1541 Massachusetts Avenue Cambridge, MA 02138 (617) 495-4500).
97. LawRelating to Right to Privacy in India – An Analysis, *available at* [https://shodhganga.inflibnet.ac.in/bitstream/10603/98806/11/11\\_chapter%204.pdf](https://shodhganga.inflibnet.ac.in/bitstream/10603/98806/11/11_chapter%204.pdf) (Last visited on June, 17, 2018).
-



98. Lee Kovarsky, “Tolls on the Information Superhighway: Entitlement Defaults for Click stream Data” (RYAN STORES et al editor) (VIRGINIA LAW REVIEW) (Vol. 89:1037) (No. 5) (4-6) (1046-1047) (2003).
99. Lee A. Bygrave and Kamiel J. Koelman, *Privacy, Data Protection and Copyright: Their Interaction in the Context of Electronic Copyright Management Systems, Copyright and Electronic Commerce, Legal Aspects of Electronic Copyright Management*, 94 (Editor, P. Bernt Hugenholtz),(2000), (Published by, Kluwer Law International Ltd., London, United Kingdom)
100. Legal Service India- Breach of Privacy and Confidentiality under Information Technology Act, 2000, available at <http://www.legalserviceindia.com/article/1288-Breach-of-privacy-&-Confidentiality-.html> (Last visited on August 23, 2018).
101. Lewis Morgan, “Hacking v Unauthorised access-What’s the difference?” (26<sup>th</sup> June 2015), available at <https://www.itgovernance.co.uk/blog/hacking-vs-unauthorised-access-whats-the-difference/> (Last visited on August 10, 2018).
102. Madhavi Divan, “The right to privacy in the age of Information and Communication”, (2002) 4 SCC J-12, available at <https://www.sconline.com/Members/SearchResult.aspx> (Last visited on February 21, 2020).
103. Mehrdad Ghayoumi, “Review of Security and Privacy Issues in e-Commerce”, available at [http://worldcomp\\_proceedings.com/proc/p2016/EEE6029.pdf](http://worldcomp_proceedings.com/proc/p2016/EEE6029.pdf) (Last visited on June 8, 2017).
104. MIT (Massachusetts Institute of Technology) Technology Review, available at <https://www.google.co.in/search?q=MIT&oq=MIT&aqs=chrome...69i57j69i61j0l4.1351j0j7&sourceid=chrome&ie=UTF-8> (Last visited on 04.10.2018).
105. Ms. Palak Gupta and Dr. Akshat Dubey, *E-Commerce- Study of Privacy, Trust and Security from Consumer’s Perspective* 224-232 (Vol.5 Issue 6, June) (2016), available at <http://www.ijcsmc.com/docs/papers/June2016/V5I6201647.pdf>, (Last visited on June
106. Ms. Talat Fatima, “Privacy on the Web” 23 (Vol.1) 2005 *CLC1 (Mad) CLC 273 (Delhi)* (Shri D. Varadarajan Edtr.)(2005).
-

107. Na. Vijayashankar, *Cyber Laws, for every Netizen in India with Information Technology Bill99* 149, (1<sup>st</sup> Edn. 1999, December), (Publishers, Ujvala Consultants Pvt. Ltd, Bangalore-560050. India.).
  108. Nandan Kamath, *Law Relating to Computers, Internet & E-Commerce* 292 (Foreword by N.R. Madhava Menon) (Universal Law Publishing) (LexisNexis) (Fifth Edition 2012) (Reprint 2016).
  109. Nandan Kamath, *Personal Data Privacy in the Online Context, Law Relating to Computers Internet & E-Commerce, A Guide to Cyber laws & The Information Technology Act, Rules, Regulations and Notifications along with Latest Case Laws* 305 (Universal Law Publishing, LexisNexis 5<sup>th</sup> Edn., Reprint, 2016).
  110. Niharika Vij, *Law & Technology* 32 (Foreword by Dr. Lalit Bhasin) (Universal Law Publishing, Co. Pvt. Ltd) (2005).
  111. Nimish Vartak, Anand Patwardhan, *et.al*, “Protecting the Privacy of Passive RFID tags”, *available at* <https://pdfs.semanticscholar.org/2b44/c877d53d27ebc4a0f810f562000a28813794.pdf> (Last visited on October 3, 2018).
  112. NS Nappinai, *Cyber Laws Part II: A guide for victims of cyber crimes*, *available at* <https://economictimes.indiatimes.com/tech/internet/do-you-know-how-to-report-a-cyber-crime-heres-a-guide-for-victims/articleshow/61464084.cms?from=mdr> (Last visited on 24/09/2019 at 2:35 PM).
  113. OECD Principles, *KnowledgEquity* (Published Mar. 16, 2016), *available at* <https://www.youtube.com/watch?v=T8rMS2nKMmI> (Last visited on October 6, 2018).
  114. The OECD Privacy Framework, *available at* [https://www.oecd.org/sti/ieconomy/oecd\\_privacy\\_framework.pdf](https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf) (Last visited on February 11, 2019).
  115. PATRIOT Act, (*Encyclopedia Britannica*), *available at* <https://www.britannica.com/topic/USA-PATRIOT-Act> (Last Visited on January 21, 2020).
  116. Paul A. Watters, *Taming the Cookie Monster* (2012), *available at* <http://www.canberra.edu.au/cis/storage/Taming%20the%20cookie%20monster-%20FINAL.pdf> (Last visited on June 22, 2017).
-

117. Pavan Burugula and Advait Rao Palepu, *available at* [https://www.business-standard.com/article/markets/sebi-to-come-up-with-special-policy-to-ensure-data-privacy-for-investors-118082600515\\_1.html](https://www.business-standard.com/article/markets/sebi-to-come-up-with-special-policy-to-ensure-data-privacy-for-investors-118082600515_1.html) (Last visited January 18, 2020).
118. Paven Duggal, (2000), *available at* <http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan002090.pdf> (Last visited on June 22, 2017).
119. Pen register, Available at *available at* [https://en.wikipedia.org/wiki/Pen\\_register](https://en.wikipedia.org/wiki/Pen_register) (Last visited on July 23, 2018).
120. Personal Information, Available at *available at* <https://www.google.com/search?q=2011+amendment+act+of+I.T.+Act&oq=2011+amendment+act+of+I.T.+Act&aqs=chrome.69i57j33.12322j0j7&sourceid=chrome&ie=UTF-8> (Last visited on July 23, 2018).
121. Peter B. Maggs, John T. Soma et al *Internet and Computer Law* 634 (Printed in the United States of America) (2001).
122. Peter Carey, *Data Protection in the U.K.* 4 (Published by the Blackstone Press Limited, 2000).
123. Peter P. Swire, *of Elephants, Mice, and Piracy: the international Choice of Law and the Internet* 32 (International Law 991, 1016 1998).
124. Prashant Mali *Cyber Law & Cyber Crimes* 2, Information Technology Act, 2000 With New IT Rules, 2011.
125. Pratik Bhakta “*Insists on local storage of data, Paytm tells govt.*” (July 24, 2018), *available at* <https://economictimes.indiatimes.com/small-biz/startups/newsbuzz/insist-on-local-storage-of-data-paytm-tells-govt/articleshow/65112783.cms> (Last visited on August 10, 2018).
126. Pratik Bhakta, “WhatsApp had said it uses the Facebook platform to process United Payments Interface transactions originating out of India”, (Last Updated, July 24, 2018), *available at* <https://economictimes.indiatimes.com/small-biz/startups/newsbuzz/insist-on-local-storage-of-data-paytm-tells-govt/articleshow/65112783.cms?from=mdr> (Last visited on August 10, 2018).
127. Praveen Dalal, “Data Protection Law in India: The TRIPS Perspective” (Vol. 11) March *Journal of Intellectual Property Rights*, 125-131 (2006), *available at*
-

<http://nopr.niscair.res.in/bitstream/123456789/3561/1/JIPR%2011%282%29%20125-131.pdf> (Last visited at June 28, 2019).

128. Privacy, Available at <https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/> (Last visited on July 23, 2018).
  129. Privacy Invasive, Available at [https://en.wikipedia.org/wiki/Privacy-invasive\\_software](https://en.wikipedia.org/wiki/Privacy-invasive_software) (last visited on July 23, 2018).
  130. Privacy Available at <https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/> (Last visited on July 23, 2018).
  131. Privity of Contract, *available at* <http://www.legalservicesindia.com/article/378/Privity-of-contract-&-third-party-beneficiary-in-a-contract.html> (last visited on February 13, 2020).
  132. Privacy Act of 1974, *available at* <https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1279> (Last visited on January 21, 2020).
  133. Privacy (Younger Report), 13<sup>th</sup> July, 1973, *available at* <https://www.theyworkforyou.com/debates/?id=1973-07-13a.1955.6> (last visited November 19, 2019).
  134. Prof. Dr. Ulrich Sieber, "Legal Aspects of Computer-Related Crime in the Information Society" –COMCRIME-STUDY- (Version 1.0 of 1<sup>st</sup> January 1998), *available at* <http://www.edc.uoc.gr/~panas/PATRA/sieber.pdf> (Last visited on March 29, 2019).
  135. P. Bernt Hugenholtz (ed.), *Copyright and Electronic Commerce, Legal Aspects of Electronic Copyright Management* (Information Law Series-8, Published by, Kluwer Law International Ltd, Sterling House, London Kingdom) (2000).
  136. Professor H. Snijders and Professor S. Weatherill (Eds.), *E-Commerce law: National and Transnational Topics and Perspectives* (Cyril van der Net, Civil Liability of Internet providers following the Directive on Electronic Commerce), 49, (Published by Kluwer Law International) (2003).
  137. Prof. Vimlendu Tayal, *Cyber Law, Cyber Crime, Internet and E-Commerce* 34 (Published by Bharat Law) (First Published 2011).
-

138. Raghavendra Kumar, "Right to Privacy: Juridicial Vision" 195 A.I.R. (Vol.89) (RAJ.SIK) (Acts N.O.C.) (Published by: S.W. Chitale for All India Report Pvt. Ltd.) (Printed at the Air Rotary Printing Press) (2002).
139. Raghavendra S. Srivasta and Sukruta R., "Online Contracts", *available at* <http://14.139.60.114:8080/jspui/bitstream/123456789/722/9/Online%20Contracts.pdf> (Last visited on February 13, 2020).
140. Rahul Matthan, *Privacy 3.0 Unlocking our Data-Driven Future* 15 (HarperCollins Publisher) (Printed at Thomas Press (India) Ltd.)(2018).
141. Rakesh Kumar and Ajay Bhupen Jaiswal, *Cyber Laws* 64 (APH Publishing Corporation, New Delhi) (2011).
142. Raman Mittal and Neelotpal Deka, *Cyber Privacy, Legal Dimensions of Cyberspace* 197 (S.K. Verma & Raman Mittal, Eds.), Indian Law Institute.
143. Ramnath K. Chellappa, "Consumer's Trust in Electronic Commerce Transactions: The Role of Perceived Privacy and Perceived Security", *available at* <https://pdfs.semanticscholar.org/7e2f/bad4fa4877ea3fd8d197950e335d59ebedf.pdf> (Last visited on September 8, 2018).
144. Ramesh Kumar, Right to privacy, Ph.D. Thesis, University of Allahabad (2010), *available at* <file:///C:/Users/LIBRARY/Desktop/privacy.pdf> (Last visited on November 14, 2019).
145. RBI Panel seeks rights- based data privacy protection in household finance, *available at* <https://www.thehindubusinessline.com/money-and-banking/rbi-panel-seeks-rightsbased-data-privacy-in-household-finance/article9831337.ece> (Last visited on August 8, 2018).
146. Rehana Parveen, *Protection of Privacy in India: Law and Juridical Concerns* (2010), Available at [http://shodhganga.inflibnet.ac.in/bitstream/10603/52364/1/01\\_title.pdf](http://shodhganga.inflibnet.ac.in/bitstream/10603/52364/1/01_title.pdf) (Last visited on October 1, 2018).
147. Richard Morgan & Ruth Boardman, *Data Protection Strategy, Implementing Data Protection Compliance* 90(Published by, Sweet & Maxwell, 2003, London NW3 3PF) (2003).
-

148. Right to Privacy in India, *available at* <http://www.indialawjournal.org/archives/volume7/issue-2/article3.html> (Last visited on July 22, 2017).
149. Right of Privacy and Internet *available at* [https://shodhganga.inflibnet.ac.in/bitstream/10603/58938/11/11\\_chapter%206.pdf](https://shodhganga.inflibnet.ac.in/bitstream/10603/58938/11/11_chapter%206.pdf) (Last visited on April 29, 2017).
150. Right to Privacy was also recognized in U.K. and it is evident from the introduction of ‘House of Commons Bill’ on November 26<sup>th</sup> of 1969. This Bill was introduced by the then MP Mr. Brian Walden. Other former Bills include Bills of 1961 and 1967. The U.K. Government also took initiative on ‘privacy’ protection and stated that legislation must be strengthened to provide complete privacy protections to individuals and consumers per se, Importance of Right to be ‘left alone’ and ‘Anxiety over privacy’ were also instituted in UK. ‘Anxiety UK’ is another important aspect in UK, which ensures and respect privacy of an individual, *available at* <https://www.anxietyuk.org.uk/privacy-policy/> (Last visited on October 19, 2018).
151. Rishika Taneja and Sidhant Kumar, *Privacy Law, Principles, Injunctions and Compensation* 231(EBC Publishing (p) Ltd., Lucknow) (Printed by, Gopsons Papers Ltd., A-2, Sector-64, Noida) (1<sup>st</sup> Edn. 2014).
152. Robert Gellman, “Fair Information Practices: A basic History”, *available at* <https://bobgellman.com/rg-docs/rg-FIPshistory.pdf> (Last visited on March 18, 2019).
153. Roger L. Sadler, *Electronic Media Law* 175 (Sage Publications, Inc.) (2005).
154. Rolf H. Weber and Romana Weber *Internet of Things Legal Perspectives* 43(Published by Springer-Verlag Berlin Heidelberg) (2010).
155. Ronald J. Mann, “Electronic Commerce” 303(Third Edition) (2008) (Aspen Publishers) (Printed in the United States of America).
156. Rowan Cruft, S. Mathew, *et.al.* (eds.), *Philosophical Foundations of Human Rights*.
157. Sabine Trepte and Leonard Reinecke “The Social Web as a Shelter for Privacy and Authentic living”, *available at*
-

- <https://pdfs.semanticscholar.org/b526/5e67813a5b1440c4d61a311e62a4c3328a1f.pdf> (Last visited on August 13, 2018).
158. S. Praveen Raj and Aswathy, “Comparison between Information Technology Act, 2000 & 2008”, *International Journal of Pure and Applied Mathematics* (Volume 119 No. 17 2018, 1741-1756), *available at* <https://acadpubl.eu/hub/2018-119-17/2/141.pdf> (Last visited on January 16, 2019).
159. Securities and Exchange Board of India (SEBI) defines data as information’s in structural and unstructured form collected and reported in various databases, Guidelines for seeking Data (2019), *available at* <https://www.sebi.gov.in/pdf/guidelines-of-data-sharing-final.pdf> (Last visited on February 6, 2020).
160. SEBI issues Risk Framework Guidelines, *available at* <https://www.bankinfosecurity.com/sebi-issues-risk-framework-guidelines-a-8383> (Last visited on March 23, 2019).
161. Shiv Shankar Singh, “Privacy and data Protection in India: A Critical Assessment” 663 *JL of THE INDIAN LAW INSTITUTE* (Vol. 53, 1-4, 2011) (July to September 2011) 53 *JILI* (2011) (2011).
162. .S.K. Verma and Raman Mittal (eds.) *Legal Dimensions of Cyberspaces*, 98 (ILI, Delhi).
163. Social Networking Sites privacy issues overview, (Handson ERP) (Published on Jan 8, 2014), *available at* <https://www.youtube.com/watch?v=EGIAbmTwmvk> (Last visited on August 13, 2018).
164. Spyware, Available at <https://en.wikipedia.org/wiki/Spyware> (Last visited on July 23, 2018).
165. Srivathsa Gottipati, “Exploratory Data Analysis (EDA)”, *available at* <https://medium.com/@srivathsagottipati/exploratory-data-analysis-eda-4b81d84ef5cf> (Last visited on December 16, 2019)
166. Stephen E. Fienberg “Privacy and Confidentiality in an e-Commerce World: Data Mining, Data Ware Housing, Matching and Disclosure Limitation” (11 Sep.2006), *available at* <https://arxiv.org/pdf/math/0609288.pdf> (Last visited on August 13, 2018).
167. Subhajit Basu, “Policy-Making, Technology and Privacy in India”<sup>7</sup> (NLSIU Bangalore) *Indian Journal of Law and Technology* (2010).
-

168. Sumeet Kumar Singh, "Spamming: Is It Infringement of Privacy" (p. 28) (January- March) (2011 Cri LJ 1) [All India Reporter (Pvt. Ltd)].
  169. Sundargopal Ghoshal "A Study of Legal control of Cyber\_Crimes with special reference to the Information Technology Act" (2005), *available at* [http://shodhganga.inflibnet.ac.in/bitstream/10603/64010/5/05\\_contents.pdf](http://shodhganga.inflibnet.ac.in/bitstream/10603/64010/5/05_contents.pdf) (Last visited on August 13, 2018).
  170. Suriya Begum, Sujeeth Kumar, *et al.*, *A Comprehensive Study on Ethical Hacking*, *available at* <http://www.ijesrt.com/issues%20pdf%20file/Archive-2016/August-2016/21.pdf> (Last visited on July 23, 2018).
  171. The Court in Puttaswamy case not only attempted to define the nebulous concept of 'privacy' but did analyzed the various hues and shades of 'privacy' and finally contained the myriad concept of 'privacy' within perceptible contours, *available at* <https://medium.com/indrastra/an-analysis-of-puttaswamy-the-supreme-courts-privacy-verdict-53d97d0b3fc6> (Last visited on December 19, 2018).
  172. Talat Fatima, *Cyber Crimes* 210 (EBC Publishing Pvt. Ltd.) (2016).
  173. Tatiana Balaban "Choice of law and Jurisdiction in E-commerce contracts with focus on B2C Agreements", *available at* [file:///C:/Users/hp/Downloads/balaban\\_tatiana.pdf](file:///C:/Users/hp/Downloads/balaban_tatiana.pdf) (Last visited on September 9, 2019).
  174. The International Criminal Police Organization, *available at* [https://www.un.org/sc/ctc/wp-content/uploads/2017/02/icpo\\_background-Information.pdf](https://www.un.org/sc/ctc/wp-content/uploads/2017/02/icpo_background-Information.pdf) (Last visited on March 26, 2019).
  175. T. Ramappa, *Legal Issues in Electronic Commerce* 86 (First Published 2003) (Published by Rajiv Beri for Macmillan India Ltd.).
  176. The Right to Privacy in India, (2016), Available at [https://privacyinternational.org/sites/default/files/UPR27\\_india.pdf](https://privacyinternational.org/sites/default/files/UPR27_india.pdf) (Last visited on June 22, 2017).
  177. The IT Law Wiki, *available at* [http://itlaw.wikia.com/wiki/Traffic\\_data](http://itlaw.wikia.com/wiki/Traffic_data) (Last visited on July, 2018).
  178. Theft, Available at [https://shodhganga.inflibnet.ac.in/bitstream/10603/132472/10/10\\_chapter%205.pdf](https://shodhganga.inflibnet.ac.in/bitstream/10603/132472/10/10_chapter%205.pdf) (Last visited on January 15, 2019).
-



179. T. Ramappa, *Legal Issues in Electronic Commerce* 179 (Published by Rajiv Beri for Macmillan India Ltd.) (2003).
180. The Securities and Exchange Board of India Act, 1992
181. The term ‘Privacy’ has also been divided into three strata, i.e., by physical space, by choice and by information which are personal, *available at* <https://www.ntia.doc.gov/legacy/ntiahome/privacy/files/CPRIVACY.PDF> (Last visited on September 5, 2018).
182. Tulane Law Review 1219 (May 1994).
183. Unauthorized access, Available at <https://www.computerhope.com/jargon/u/unauacce.htm> (Last visited on January 15, 2019).
184. USA: Data Protection 2019, *available at* <https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa> (Last visited on November 11, 2019).
185. Vijoy Dal Dalmia, “India: Data Protection Laws in India-Every Thing You Must Know” (Last updated: 13 Dec. 2017), *available at* <http://www.mondaq.com/india/x/655034/data+protection/Data+Protection+Law+in+India> (Last visited on January 12, 2019).
186. Vivek Sood *Cyber Crimes, Electronic Commerce & Investigation Legal Issues* 243 (Foreword by MR. Goolam E. Vahanvati & 1<sup>st</sup> edition Foreword by Mr. Justice Ajit Prakash Shah) (Published by Ajay Kumar Garg, Nabhi Publication) (2010).
187. Vivek Kumar and Dr. V.K. Gaur, “*Data Privacy in Offshore Outsourcing to India*” 32 (Corporate Law Cases, Vol.2) (2010) CLC465 (SC).
188. Vibhor Verdhan “Breach of Confidentiality and Various Legal issues”, *available at* <http://www.legalserviceindia.com/article/1413-Breach-Of-Confidentiality-&-Various-Legal-Issues.html> (Last visited on October 19, 2018).
189. White Paper on Data Protection Framework for India-Public Comments Invited, *available at* <https://meity.gov.in/white-paper-data-protection-framework-india-public-comments-invited> (Last visited on 14/03/2019).
-

190. What is GDPR, *available at* <https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018> (Last visited on January 30, 2020).
191. Why does Privacy Matter? Available at <https://www.theatlantic.com/technology/archive/2013/02/why-does-privacy-matter-one-scholars-answer/273521/> (Last visited on July 23, 2018).
192. What is the difference between the DPA, 2018 and the GDPR, *available at* <https://www.dpocentre.com/difference-dpa-2018-and-gdpr/> (Last visited on January 30, 2020).
193. Wiki Leak, Available at <http://www.dictionary.com/e/wikileaks-wikipedia/> (Last visited on 23, 2018).
194. WIPO, Intellectual Property Handbook, *available at* [https://www.wipo.int/edocs/pubdocs/en/intproperty/489/wipo\\_pub\\_489.pdf](https://www.wipo.int/edocs/pubdocs/en/intproperty/489/wipo_pub_489.pdf) (2004, 2<sup>ND</sup> Edition) (Reprinted 2008), (Last visited on March 26, 2019).
195. WTO Appellate Body Repertory of Reports and Awards 1995-2010, *available at* [https://books.google.co.in/books?id=xMNOdF7vuXkC&pg=PA267&lpg=PA267&dq=%E2%80%9Ca+responding+party+must+make+a+prima+facie+case+that+its+challenged+measure+is+%E2%80%98necessary.%E2%80%99%E2%80%9D&source=bl&ots=9CJw\\_QFWIE&sig=IgwNd88G-xIx8bBAp5PDs9JV67c&hl=en&sa=X&ved=0ahUKEwiQoaGG9szXAhURTo8KHT\\_fAzwQ6AEIJzAA#v=onepage&q=%E2%80%9Ca%20responding%20party%20must%20make%20a%20prima%20facie%20case%20that%20its%20challenged%20measure%20is%20%E2%80%98necessary.%E2%80%99%E2%80%9D&f=false](https://books.google.co.in/books?id=xMNOdF7vuXkC&pg=PA267&lpg=PA267&dq=%E2%80%9Ca+responding+party+must+make+a+prima+facie+case+that+its+challenged+measure+is+%E2%80%98necessary.%E2%80%99%E2%80%9D&source=bl&ots=9CJw_QFWIE&sig=IgwNd88G-xIx8bBAp5PDs9JV67c&hl=en&sa=X&ved=0ahUKEwiQoaGG9szXAhURTo8KHT_fAzwQ6AEIJzAA#v=onepage&q=%E2%80%9Ca%20responding%20party%20must%20make%20a%20prima%20facie%20case%20that%20its%20challenged%20measure%20is%20%E2%80%98necessary.%E2%80%99%E2%80%9D&f=false) (Last visited on November 20, 2017).
196. Yee Fen Lim, *cyberspace law* 133 (Publication Oxford University Press) (2008).
197. Yun Zhao, *Dispute Resolution in Electronic Commerce*, 143 (Martinus Nijhoff Publishers).
-