Right to privacy in Cyberspace-A Constitutional Analysis

A Thesis Submitted

To

Sikkim University

In Partial Fulfilment of the Requirement for the

Degree of Doctor of Philosophy

By

N R Rakesh Das

Department of Law

School of Social Sciences

Sikkim University

February 2024

Date:

DECLARATION

I, N R Rakesh Das, hereby declare that the research work embodied in the thesis "**Right to Privacy in Cyberspace-A Constitutional Analysis"**, submitted to Sikkim University in partial fulfilment 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.

Place: Gangtok

Date:

N R Rakesh Das

Ph.D.Registration No:

Registration Date:

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

6th Mile, Samdur, Tadong-737102
Gangtok, Sikkim, India
Ph. 03592-251212, 251415, 251656
Telefax : 251067
Website : 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)

CERTIFICATE

This is to certify that the thesis titled as **"Right to Privacy in Cyberspace- A Constitutional Analysis",** submitted to Sikkim University in partial fulfillment of the requirement for the Degree of Doctor of Philosophy in the Department of Law, embodies the result of bona fide research work carried out by Sri N R Rakesh Das under my guidance and supervision. No part of the Thesis has been submitted for any other Degree, Diploma, Association and Fellowship.

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

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

Supervisor

Dr. Nidhi Saxena
Assistant Professor
Department of Law
School of Social Sciences
Sikkim University

Head of the Department (I/C)

Dr. Denkila Bhutia
Assistant 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

6th Mile, Samdur,Tadong -737102
Gangtok, Sikkim, India
Ph. 03592-251212, 251415, 251656
Telefax: 251067
Website: 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)

PLAGIARISM CHECK CERTIFICATE

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

"Right to Privacy in Cyberspace- A Constitutional Analysis"

Submitted by Sri N R Rakesh Das under the supervision of Dr. Nidhi Saxena, Assistant Professor, Department of Law, Sikkim University, Gangtok, Pin: 737101, India.

Signature of the Scholar

(N R Rakesh Das)

Counter Signed by the Supervisor

(Dr. Nidhi Saxena)

केन्द्रीय पुस्तकालय Central Library
सिक्किम विश्वविद्यालय
SIKKIM UNIVERSITY

Verified by Librarian

CONTENTS

Page No

CHAPTER 5: Data Protection, Regulations, Policies and Principles in Europe, and India.

CHAPTER 6: Conclusion and Suggestion.

ACKNOWLEDGEMENT

Date: 22/02/2024

Right to privacy in Cyberspace-A Constitutional Analysis My research journey has been the most enriching and beautiful journey that I have covered to date, and with the generous blessings, support and assistance of numerous people, my thesis became a reality. It gives me great pleasure to thank each and every one of them. I would like to start by expressing my gratitude to my supervisor, Dr. Nidhi Saxena, an assistant professor in the law department at Sikkim University, for her skilful guidance, insightful teachings, and emotional support. I am grateful for her loving demeanor in this hour of challenging circumstances. She has been and will continue to be a mentor and inspiration to me.

I humbly thank The Honorable High Court of Tripura for granting me the opportunity to peruse my Research Work. I humbly thank Honorable Mr. Justice Aparesh Kumar Singh, Honorable Chief Justice of Tripura, Honorable Mr. Justice Indrajit Mohanty, Honorable Chief Justice of Tripura (Retired), Honorable Mr. Justice Subhasis Talapatra, Honorable Chief Justice of Orissa (Retired), Honorable Mr. Jutice Arindam Lodh, Honorable Judge High Court of Tripura, Honorable Mr. Jutice T. Amarnath Goud, Honorable Judge High Court of Tripura, Honorable Judge High Court of Tripura, Honorable Mr. Justice Sabyasachi Datta Purkayastha, Honorable Judge High Court of Tripura, Honorable Mr. Justice Biswajit Palit, Honorable Judge High Court of Tripura, Sri Data Mohan Jamatia, Honorable Registrar General High Court of Tripura (Retired), Sri V Pandey, Honorable Registrar General High Court of Tripura for their parental guidance and for motivating me to pursue the path of Knowledge.

I would like to express my sincere gratitude to Professor Dr. Praveen Mishra, Head of the Law Department, for his guidance and assistance throughout my research. Additionally, I would like to thank Dr. Veer Mayank, Dr. Sonam Yangchen Bhutia, and Dr. Denkila Bhutia,

the faculty members of the Department of Law, for their unwavering support and encouragement.

Words will fall short to describe how grateful I am towards my Parents who have continuously supported me throughout this Journey. I whole heartedly thank my Father Sri Ranjit Das, my mother Smt. Kajal Saha, My Aunt Smt. Rama Saha and Smt. Bijali Saha, my Uncle Sri Sunil Saha, my wonderful Brothers and sisters for always motivating me for pursuing my dreams and for diving me wings of hope to live those dreams. I also thank Dr. Jayanta Dhar Assistant Professor NLU Tripura for his kind help and assistance. I humbly thank my brother Judges Sri Amlan Mukherjee, Sri Sushoban Das and Sri Farhad Islam for always cheering me to pursue this Course of Journey. I extend my sincere gratitude towards my friend Miss Sushma kharka, Miss Sharmistha Sigdel, Sri Shivasish Pradhan, Sri Sonam Phuntsho, Miss Nisha Rai, Miss Dichen Lama, Smt Priyanka Banik, Smt Barna majumder, Miss Sujata Sur, Sri Bittu Debnath, Sri Goutam Das and specially Miss Sushmita Majumder for their kindness and love. I also extend my sincere gratitude to Sri Tapan Das and Sri Rajesh Singha for always being my helping hand in need.

Without the infrastructure support from Sikkim University, my thesis would not be possible, and I sincerely thank the university's library staff. I owe a great deal to the different authors, jurists, and others whose writings and works I have used as inspiration to finish my work.

ABBRAVIATIONS

ABDM	**The Ayushman Bharat Digital Mission**
AEPD	**Agencia Espanola de Protecci on de Datos**
AI	**Artificial Intelligence**
AKA	**Also known As**
APEC	**Asia-Pacific Economic Cooperation**
API	**application programming interface”**
APP	**Application**
AU	**African union**
B2C	**Business to Customer**
BLAPL	**Bail Application**
CA	**Cambridge Analytica**
CalOPPA	**California Online Privacy Protection Act**
CCPA	**California Consumer “Privacy” Act**
CISOs	**Chief information security officers**
CMS	**Central Monitoring System**
CNIL	**Commission Nationale de L'informatique et des Libertés”**
COPPA	**The Children's Online Privacy Protection Act**
CPA	**Colorado “Privacy” Act**
CPRA	**California “Privacy” Rights Act**
ECJ:	**European Court of Justice**
DoS	**Denial of service**
DPA	**Data Processing Agreement**
DPD	**Data Protection Directive**
DPDP	**The Digital Personal Data Protection**
EC	**Economic Council**
ECHR	**European Convention on Human Rights**
ECJ	**European Court of Justice**

ECPA	**Electronic Communications Privacy Act**
ECtHR	**European Court of Human Rights**
FIA	**Fédération Internationale de l'Automobile**
FTC	**Federal Trade Commission**
GDH	**Gross Domestic Happiness**
GDP	**Gross Domestic Product**
GDPR	**General Data Protection Regulation**
GLBA	**Gramm-Leach-Bliley Act**
HIPAA	**Health Insurance Portability and Accountability Act**
IBM	**International Business Machines**
ICCPR	**International Covenant on Civil and Political 16 Rights**
ICICI	**Industrial Credit and Investment Corporation of India**
ICMR	**The Indian Council of Medical Research**
ICO	**Information Commissioner's Office**
ID	**Identity**
IDPR	**Inter-Domain Policy Routing**
IDS	**intrusion detection system**
IoT	**Internet of Things**
IP	**Internet protocol**
IPR	**Intellectual property rights**
IRCTC	**Indian Railway Catering and Tourism Corporation**
IT	**Information Technology Act**
LGPD	**Law of Personal “Data Protection” in Brazil**
LLC	**Logical Link Control**
MitM	**Man-in-the-Middle**
MP	**Member of Parliament**
MSMEs	**Micro, Small, and Medium Enterprises**
NCSC	**National Cyber Security Centre**
NGT	**National Green Tribunal**
NIA	**National Investigation Agency**

NPD	**Non Personal Data**
OECD	**Organisation for Economic Co-operation and Development**
PCI-DSS	**Payment Card Industry Data Security Standard**
PIPEDA	**Personal Information Protection Act**
PUCL	**People's Union for Civil Liberties**
R.B.I.	**Reserve Bank of India**
RaaS	**Ransom ware-as-a-Service**
RIPA	**Regulation of Investigatory Powers Act 2000**
RTI	**Right to Information**
SCA	**Software Composition Analysis**
SEBI	**Securities and Exchange Board of India**
SHIELD	**Stop Hacks and Improve Electronic Data Security**
TJX	**TJX Companies, Inc**
U.S.	**United States**
UDHR	**Universal Declaration on Human Rights**
UIDAI	**Unique Identification Authority of India**
UK	**United Kingdom**
UN	**United Nations**
UOI	**Union of India**
UPI	**United payment interface**
USA	**United States of America**
VPN	**Virtual Private Network**
W.P.	**Writ Petition**
WWW	**World Wide Web**

Executive Summary

This thesis is divided into six chapters and highlights various aspects that are covered in the research work.

The first chapter 'Introduction' details the problem of the study in the area of "Right to Privacy In Cyber Space- A Constitutional Analysis". This chapter also provides the research objectives, research questions, the methodology adopted and various literatures that were reviewed for the study.

The second chapter "Conceptual Framework of Right to Privacy" elaborative discusses about the process of judicial activism of How "Right To Privacy" was acknowledged as a part of Constitution. This chapter further analyses about the requirement of acknowledging "Right to Privacy" as a basic feature of contemporary constitutionalism. In this chapter I have also drawn a comparative analysis on the topic-How the global nations views the "Right To Privacy" as a part of their constitution and what steps they have taken to protect this Right. Apart from these the legal and administrative issues are also discussed in this chapter.

The Third Chapter "The Right to be forgotten: a rightful challenge against the Internet" emphasises on the issue of why Right to be forgotten is important in the era of AI and Superfast Internet. This chapter also draws a comparative analysis of different legislations which has demarcated a borderline between Right to Privacy and Right to be forgotten. Within this chapter I have also tried to address the ever-lasting dispute between Right to Privacy and Right to Information. Finally I have also analyzed the contours of "Article 21" which grants a scope to include "Right to be Forgotten" as a part of this grand norm.

The Fourth Chapter “Data Privacy and Protection of Personal Data in India” deals with the elaborative analysis of Indian policies which the Indian Legislators had adopted throughout the course of time to ensure proper protection of sensitive information of its citizens. With the progression of this chapter I have tried to put some light on the Legal and economical impact over the world due to loss of Data by way of data breach and I have also suggested probable ways to tackle these issues. Finally the fourth chapter concludes with the in-detail study of the point that the standard form of e-contracts which are issued by data fiduciaries does not qualify to reach the standards of free prior in formed consent necessary for e-contracts.

The Fifth Chapter deals with Data Protection Regulations, Policies, and Principles in Europe, and India. In this chapter I have discussed about various kinds of cyber attacks which has been inflicted upon the global citizens. To describe the situation better many case studies has been discussed in this chapter. Finally the chapter comprehensively studies the point that Privacy can be managed by an Individual provided proper scope is given to an individual for developing the sense of privacy.

The last chapter ‘Conclusion and Suggestion’ summarizes the entire study and provides suggestions after analysing every aspect of the work. An attempt has been made to point out inadequacy of existing legislation in connection with privacy laws and the rights of citizens. Likewise, various suggestions have been provided to deal with this.

CHAPTER 1

Right to "Privacy" in Cyberspace-A Constitutional Analysis

Introduction:

"Privacy is not something that I am merely entitled to, it is an absolute prerequisite."
- Marlon Brando

In today's world data has become so available that if you purchase a packet of potato chips, 2 giga bytes worth of data can be included in your existing data pack, and we being the citizen of Social media, have happily accepted that deal. However, it is a matter of concern that, by implementing this short marketing policy the producers of that particular chips brand and the service provider of that particular internet franchise are able to control our consumer behavior and gather important information necessary for launching future products. This may sound so simple, but is very important for the existence of our "Right to Choose".

The "Concept of right" has been acknowledged by many scholars as the most important ingredient for the ultimate development of a person and his intellectuality. Among such rights, "the right to "Privacy"" is considered the important rights essential to establishing one's identity in a community. The Merriam- Webster dictionary defines the term '"Privacy"' as the quality or state of being apart from company or observation and the freedom from un-authorized intrusion[1]. As the definition suggests, "Privacy" is a right in rem which provides a person the authority to conceal any knowledge/ data which he/she doesn't want to share with any other person. "Privacy", according to Judith Thomson[2], is a collection of derivative rights, some of which are derived from the right to own or use one's property, others' rights to

[1] Definition of "PRIVACY", , https://www.merriam-webster.com/dictionary/"Privacy" (last visited Oct 16, 2021).
[2] Judith Jarvis Thomson, *The Right to "Privacy"*, 4 PHILOSOPHY & PUBLIC AFFAIRS 295–314 (1975), http://www.jstor.org/stable/2265075.

one's person, the autonomy to control one's body, and so forth. Thomson observes that "there is no such thing as violating a man's right to "Privacy" by simply knowing something about him," she justifies this with the argument that "None of us has a claim over any fact to the consequence that fact shall not be known by others." If knowing something about you violates your "right to "Privacy"", it must be due to the method by which the truth was discovered; "it is about the how, not the what", that is known about you. In the era of internet, where data is valued as the new liquid gold, it is quite challenging to insure proper security to one's personal data. For instance Cambridge Analytica "Data Breach"[3], Yahoo "Data Breach" in 2013-14 impacting 3 Action users[4], LinkedIn "Data Breach" in 2021 which saw a massive data loss of 700 million users[5] has brought the necessity for strong and comprehensive sui generis data "Privacy" regulations for both domestic and international platforms to the attention of global populations.

One may ask, why the global community has a certain need of "Data Protection" policy in cyberspace or in any other platform? To answer this question, let us play a game of presumption. Imagine a world, where no walls or boundaries exists, everything is visible, audible to everyone. Everything that we do can be seen by others, and every word that we utter can be heard. In short our "Privacy" is locked away in a panopticon. In modern world where everything is connected via world wide web, and our social, financial and political information are being stored in a cloud storage or a server, in such a situation nothing can be truly identified as private. We may conclude that the need for a working "Data Protection"

[3] Julia Carrie Wong, *The Cambridge Analytica scandal changed the world – but it didn't change Facebook*, THE GUARDIAN, March 18, 2019, https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook (last visited Oct 17, 2021).

[4] The Hacked & the Hacker-for-Hire: Lessons from the Yahoo "Data Breach"es (So Far), , THE NATIONAL LAW REVIEW , https://www.natlawreview.com/article/hacked-hacker-hire-lessons-yahoo-data-breaches-so-far (last visited Oct 17, 2021).

[5] LinkedIn denies "Data Breach" that reportedly affected 700 million users, THE ECONOMIC TIMES, June 30, 2021, https://economictimes.indiatimes.com/tech/technology/amazon-owned-twitch-says-source-code-exposed-in-last-weeks-data-breach/articleshow/87057155.cms (last visited Oct 17, 2021).

law is real and not just a gimmick because the world is gradually realizing how important this is.

Data "Privacy" in India:

The common law gives each person the freedom to choose, in most cases, how much of his thoughts, feelings, and emotions are shared with others (Yates, J., in Millar v. Taylor, 4 Burr.2303, 2379 (1769))[6]. India's digital adventure has been exhilarating. In 2020, the country has the second-largest internet population in the world, with over 749 million users. Mobile phones were used by 744 million people to access the internet. Estimates suggest that by 2040, this number will have risen to almost 1.5 Action[7]. With the ease of internet domestic businesses are blooming, new methods of digital payment systems are getting introduced, trade in crypto currencies are taking place, and last but not the least even babies won't take food without the active stimulation of cartoons in YouTube. All of these are happening with the least concern about the least concern for one's private data. To state that India's Gross Domestic Happiness (GDH) is heavily reliant on the Internet and other online service providers would not be incorrect. As I have mentioned earlier data is the modern day currency for global trade. The importance of data can be best described through the examples of Technological Giants like Alphabet, Facebook, Twitter etc. Have we ever thought of, why is it such that, whenever we download an application from Play store or Apple store, we have to agree to their "Privacy" policy and cannot proceed further without the confirmation? The reason behind such "Privacy" policy is, the tech giants wants to collect user data to understand individual customer choices which will help their subsidiaries or other stakeholders to target their customers and sell personalized products. For an example: During

[6] "It is certain every man has a right to keep his own sentiments if he has certainly a right to judge whether he will make them public or commonly to the sight of his friends" Yates, J., in Millar v. Taylor, 4 Burr. 2303, 2379 (1769).

[7] Sandhya Keelery, India: Mobile internet users, , STATISTA , https://www.statista.com/statistics/558610/number-of-mobile-internet-user-in-india/ (last visited Oct 17, 2021).

Festive seasons, whenever we open google, other search engines, any websites or even government handled applications like IRCTC we are likely to find adds showcasing items of our interest (Like Apparels, Electronic Gadgets). In short we are a generation who cannot complete our day without internet, our day to day needs, transportation, health care, insurance, housing, entertainment, relationships are largely dependent on Internet. The matter of concern out here is, our primary focus is on maintain this lifestyle and we are least concerned about our private data and the way how service providers are collecting these data to influence our Right to Choose. “The Indian Constitution” does not make “the right to Privacy” clear or explicit; instead, courts have had to interpret it. Through judicial interpretation, “The Right to Privacy has been acknowledged as a part of Fundamental Right” .The ability to “Privacy” in Indian law dates back to the late 1800s, when a British local court upheld a pardanashin woman's ability to go to her balcony without worrying about being seen by neighbouring people. Although the Indian Constitution does not specifically guarantee the right to “Privacy”, jurisprudence has grown since that right was recognized under “Article 21” of the document.

Literature Review:

1. **Jed Rubenfeld[8]:** In this article the author takes us on a journey of understanding the "right to "Privacy"". He has given a detailed analysis on a process of 'right to "Privacy"' becoming a part of the basic "fundamental right". "Privacy" being one of the key ingredient of one's personhood, the sovereign must give it a chance to bloom. The concept of "Privacy" is used to regulate the actions of others who encroach on one's life in numerous ways. In these circumstances, "Privacy" can be broadly defined in the conventional informational sense: it restricts others' ability to get, transmit, or use information about oneself. The right to "Privacy" that we are concerned about, on the other hand, is linked to the rightholder's own conduct. It is substantive rather than informative, and it protects from unwelcomed particular intruders.

2. **M.T. Dlamini, H.S. Venter, J.H.P. Eloff, and M.M. Eloff[9]:** When it comes to defining "Privacy", there are numerous options. Everything relies on how one interprets the idea of "Privacy". Most of the approaches are integrative, individualistic, and structuralist. From a structuralist perspective, "Privacy" is defined in the norms of social structures. It includes the "moral and legal right" to limit the access that others have to specific information or individuals. The authors have emphasized the importance of creating a strong "Data Protection" system and have stated that in the era of ubiquitous information sources, phony news, fake social media profiles, and fake digital identities are all examples of falsified online content that can be grouped together as digital deception.. *(Need for a "Data Protection" laws)*

[8] Jed Rubenfeld, *The Right of "Privacy"*, 102 HARVARD LAW REVIEW 737–807 (1989), https://www.jstor.org/stable/1341305 (last visited Oct 24, 2021).
[9] M. T. Dlamini et al., *Digital deception in cybersecurity: an information behaviour lens* (2020), http://informationr.net/ir/25-4/isic2020/isic2018.html (last visited Oct 18, 2021).

3. **Jerry Kang[10]:** The author starts with a brief description of cyber space and the role that cyber space plays in our social, economic and political activities. He further draws our attention towards the importance of "Data Protection" in the ever growing industry of e-transaction, as many of our data are beyond our control or mostly we are unware of 'information business' that has been carried on by different stakeholders in service provider industry. He has rightly pointed that, to ensure data "Privacy" in cyber space both the private and public players must actively participate tackle the techno legal gaps and address them jointly.

4. **Monique Mann, Angela Daly, Michael Wilson, Nicolas Suzor[11]:** The authors has adopted the ideology that, Nations who want to enlarge the scope of Digital constitutionalism should try to ensure freedom of internet and safeguard essential human rights, including "The "Freedom of Speech"" and expression, the right to assemble, and the right to "Privacy" online. Additionally, they propose that since the internet links us all over the world, "Data Protection" and "Privacy" policies ought to address both national and international laws. Further, these norms should be consistent with digital constitutionalist norms of "Privacy" and security.

5. **Kristian P. Humble[12] (States responsibility to protect Individual Right):** In this article the author justifies that, in the age of global communication outreach '"Privacy"' is seldom acknowledged or respected by public or private stakeholders as a 'right'. The

[10] Jerry Kang, *Information "Privacy" in Cyberspace Transactions*, 50 STANFORD LAW REVIEW 1193 (1998), https://www.jstor.org/stable/1229286?origin=crossref (last visited Oct 18, 2021).
[11] Monique Mann et al., *The limits of (digital) constitutionalism: Exploring the "Privacy"-security (im)balance in Australia*, 80 INTERNATIONAL COMMUNICATION GAZETTE 369–384 (2018), https://doi.org/10.1177/1748048518757141 (last visited Oct 19, 2021).
[12] Kristian P. Humble, *International law, surveillance and the protection of "Privacy"*, 25 THE INTERNATIONAL JOURNAL OF HUMAN RIGHTS 1–25 (2021), https://www.tandfonline.com/doi/full/10.1080/13642987.2020.1763315 (last visited Oct 21, 2021).

author strengthens his argument with the examples of Cambridge Analytica and Edward snowden. As we read the paper, it becomes clear that the author is making two points. First, she argues that states are required by contemporary international law to respect their citizens' right to “Privacy” and refrain from interfering without a valid reason. This justifiable reason falls under the purview of the "effective control test." According to the second argument, to guarantee several aspects of “Privacy”, including the right to “Privacy”, citizens' control over personal data, personhood, personality, uniqueness, and dignity, the state should strictly abide by international laws and norms. States should, however, be permitted to intercept communications to a restricted degree if there are dangers to public safety and order, and the government should decide whether to use controlled surveillance.

6. **Raymond Bierens, Bram Klievink, Jan van den Berg[13]:** In this article the authors tries to attract our attention towards the ever changing world of cyber space. According to them Cyber risks arise as a result of today's increasing connectivity on a personal, organizational, and societal level. Social media threats need to be reduced by a variety of players, with the government taking the lead, as it is the government's duty to safeguard its people. Every nation should start its governmental duties at the national level since there is no official global governance. Effective management of worldwide cyber threats is a difficult issue that requires appropriate alignment between these sovereignty formed policies. The first stage in achieving alignment is to gain knowledge into the disparities across national cyber plans. As the social contract theory mentions, the sovereign has a key role in framing policies which will impact the life of a

[13] Raymond Bierens, Bram Klievink & Jan van den Berg, *A Social Cyber Contract Theory Model for Understanding National Cyber Strategies*, 10428 *in* ELECTRONIC GOVERNMENT 166–176 (Marijn Janssen et al. eds., 2017), http://link.springer.com/10.1007/978-3-319-64677-0_14 (last visited Oct 21, 2021).

commoner, According to this idea, in the modern world, the government and IT corporations that provide Internet services have a combined responsibility to preserve citizens' "Privacy" and are strictly liable for any breaches that result from their carelessness.

7. **Scott J. Shackelford, Scott Russell, and Andreas Kuehn[14]:** In the age of modern technologies we all are global citizens, borders created by men has fallen short, as the Internet provides enough space for everyone to share a common ground. But this territory is no longer uncontested. As communication technology advanced, malicious online users were able to amass a weaponry strong enough to demolish peace in cyberspace. These kinds of threats are gradually arising day by day, the rising number of credit and debit card scams, identity thefts, ransomware attacks are perfect examples of such incidents. Due to the novelty of such incidents citizens are seldom prepared for such incidents. Stakeholders including the domestic government, service providers, and international authorities have a duty to recognize the gravity of the situation and work toward a proactive framework that considers the shared but distinct obligations of public and private sector actors in cyberspace.
8. **Dr. Axel Freiherr von dem Bussche, and Paul Voigt[15]:** There is no border for data, the nature of data allows it to travel through any country without any restriction. As, data has been identified as the next generation of currency, every stake holder in data business wishes to keep themselves a step ahead compared to another stakeholder. This kind of competition has resulted into data piracy, unethical means of data harvest and violation of data "Privacy". However, as data is the key ingredient of global economy,

[14] Scott J. Shackelford, Scott Russell & Andreas Kuehn, *Defining Cybersecurity Due Diligence Under International Law: Lessons from the Private Sector*, *in* ETHICS AND POLICIES FOR CYBER OPERATIONS 115–137 (Mariarosaria Taddeo & Ludovica Glorioso eds., 2017), http://link.springer.com/10.1007/978-3-319-45300-2_8 (last visited Oct 22, 2021).

[15] PAUL VOIGT & AXEL VON DEM BUSSCHE, THE EU GENERAL "DATA PROTECTION" REGULATION (GDPR) (2017), http://link.springer.com/10.1007/978-3-319-57959-7 (last visited Oct 23, 2021).

and businesses will fall apart without adequate data fuel, it is of utmost importance that countries should establish a harmony between data flow and data "Privacy". EU being an early member of data "Privacy" club has already established a set of rules to control data flow inside its border and outside its borders. Similarly, many developed nations have also walked on the same path. Although, uniformity in "Data Protection" norms has always been an apple of discord as countries despite having a same goal of protecting the "Privacy" of their citizens failed to create a same ground of interest to implement the laws. However, all of these are in the chapters of history now, the current situation is different and relatively dangerous, data pirates have developed numerous technologies to dive deep inside data mines, it is the need of the hours for all and sundry to come together and create universal uniform "Data Protection" norms to ensure smooth flow of data throughout the world.

9. **Christiane Wendehorst[16]:** Artificial Intelligence is one of the greatest inventions of modern science. Who could have thought that machines can also develop conscience in them? With the development of modern science, possibilities are there that, one day AI will be able to take run multiAction dollar industries on their own, all thanks to machine learning. With so much possibilities, liabilities too co-exist. The author through her analysis tries to draw our attention to the question that, should AI be strictly liable for its actions? As we know, AI or any kind of self-learning technologies hugely depends upon data to carry out their functions. For example, Tesla uses user data, compile them with real time google map feed and use them to drive the self-driving cars. Without this data, the car wouldn't move. Now, the question remains, to what extent data can be shared with AI? This question is followed by another question, how much of user data can AI

[16] Christiane Wendehorst, *Strict Liability for AI and other Emerging Technologies*, 11 JOURNAL OF EUROPEAN TORT LAW 150–180 (2020), https://www.degruyter.com/document/doi/10.1515/jetl-2020-0140/html (last visited Oct 24, 2021).

share with its parent company, and how much of data can the parent company share with other stake holders? The chain seems to grow larger. The question further gets stronger, who should be liable for any kind of "Data Breach"? Because there will be so many stakeholders, will it be difficult to determine the breaching point? The author further reiterates that, it is high time to decide upon strong guidelines to check such situation in case any occurs.

10. **Atul Singh[17]:** The authors accurately state that protecting personal data requires striking a balance between data security and the rights accorded to the individual identified by the data. While data security is an important aspect of "Data Protection" that is addressed by laws dealing with the protection of electronic data storage and processing resources, other important aspects of "Data Protection", such as an individual's right to be informed and his prior approval for data collection, processing, and sharing, data quality, and remedies available to the individual as a result of these rights, are frequently overlooked. In India, statutory "Data Protection" is not limited to information technology regulations. Other laws exist that secure important features of "Data Protection", even if such protection is secondary to their primary goal. Recognizing the legal provisions ensuring such rights and analyzing the procedures in place to ensure their execution could be the first step toward ensuring optimal "Data Protection" under existing laws and, eventually, establishing a comprehensive "Data Protection" strategy.

[17] Atul Singh, *"DATA PROTECTION": INDIA IN THE INFORMATION AGE*, 59 JOURNAL OF THE INDIAN LAW INSTITUTE 78–101 (2017), https://www.jstor.org/stable/26826591 (last visited Oct 23, 2021).

11. **Nir Kshetri[18]:** As the world is approaching towards the new heights of technological summits, tech giants has taken serious cognizance towards protecting their consumers data against any kinds of threat. To ensure maximum security stake holders in data business are adapting the use of Block chain. The author further develops four arguments to support block chain technologies use for various purposes. Firstly he suggests that regulating authorities can suggest public and private stakeholders to introduce block chain enabled supply chain management and establish the necessary guidelines for the same, secondly training key stakeholders and expanding investment in block chain technology should be the emphasis of public policy activities aimed at ensuring "Privacy" with this technology, thirdly turning your attention to public–private collaborations is one strategy to improve the block chain ecosystem, and finally national governments should give legal certainty and additional information to parties interested in engaging in enforceable smart contracts. These gaps if filled can boost up the data "Privacy" protection regime.

12. **Yanfang Wu, Tuenyu Lau, David J. Atkin, Carolyn A. Lin[19]:** Online "Privacy" refers to the approach that can be implemented over time to secure the identity of people who use the internet to gather information or express their thoughts. Users can, of course, opt not to expose their identities in an ideal online environment. However, with the growth of technologies that may detect a user's identity, legislators are wrestling with challenges around personal "Privacy" protection. Given the growth of global e-commerce, telecommuting, and other economic engines driving the global information

[18] Nir Kshetri, *Blockchain's roles in strengthening cybersecurity and protecting "Privacy"*, 41 TELECOMMUNICATIONS POLICY 1027–1038 (2017), https://linkinghub.elsevier.com/retrieve/pii/S0308596117302483 (last visited Oct 23, 2021).

[19] Yanfang Wu et al., *A comparative study of online "Privacy" regulations in the U.S. and China*, 35 TELECOMMUNICATIONS POLICY 603–616 (2011), https://linkinghub.elsevier.com/retrieve/pii/S0308596111001017 (last visited Oct 23, 2021).

economy, the stakes in this continuing policy dispute are significant. In this literature the authors have described the differences between "Data Protection" policy of a democratic nation and an authoritarian nation by analysing a comparative study between USA and China. The authors while quoting "Gibson- The internet is transnational. Cyberspace has no borders,'' states that Personal data and "Privacy" are under unprecedented threat internationally as telematics continues to spread. People now have access to global information and vice versa (individual information is open to the world) because to technological advancements. The writers have made note of the fact that in certain totalitarian nations, the government in power actively controls the media and supports state-sponsored internet surveillance in an effort to preserve public confidence. Adding salt to the injury, service providers too play the role of accomplice leaving behind their corporate social responsibility. However the situation is comparatively better in democratic countries, as free press/media exists in such counties. The authors have rightly identified the need of a global data "Privacy" norms to bring the data piracy issues in the lime light and find a fitting solution to answer the crisis.

13. **Kinfe Micheal Yilma[20]:** Through the avenues of this literature the author draws our attention to the point that, ideological and political differences among global leaders has continued to be a bolder on the path of achieving an uniform data "Privacy" law for the whole world. It takes references of Human right conferences and treaties hosted during the cold war era, which took serious blows to the ideological difference. The author goes on to say that the United Nations' present data "Privacy" regulations do not adequately uphold the concept of authentic individualistic data "Privacy". The current

[20] Kinfe Micheal Yilma, *The United Nations data "Privacy" system and its limits*, 33 INTERNATIONAL REVIEW OF LAW, COMPUTERS & TECHNOLOGY 224–248 (2019), https://www.tandfonline.com/doi/full/10.1080/13600869.2018.1426305 (last visited Oct 24, 2021).

system in place to preserve data “Privacy” has several shortcomings. These restrictions are both normative and institutional. The current framework's normative restrictions are mostly three in character. One is the 'problem of normative dispersion,' in which existing data “Privacy” standards are a patchwork of rules scattered across numerous instruments, reducing their accessibility and hence effectiveness. Second, existing data “Privacy” laws are enshrined in a plethora of soft law instruments, It has worsened their practical utility as well as diminished their normative power. Third, existing UN data “Privacy” standards are normatively inferior to regional counterparts, resulting in a limited amount of desirable protection. Added to these, there exists two more institutional deficiencies. The lack of defined institutional arrangements is its main flaw. The monitoring task lies on multiple authorities due to the dispersed nature of existing regulations. The institutional setup for monitoring existing data “Privacy” requirements is as disjointed as the regulations themselves. Another institutional shortcoming is that the multiple agencies entrusted with overseeing the various data “Privacy” standards are not equipped to implement the regulations and guarantee that they are observed. Since the majority of developing and less developed countries heavily rely on UN guidance when formulating their own domestic policies, the UN must fundamentally alter its current data “Privacy” policy to lead and assist the entire world.

14. **Debasis Bandyopadhyay and Jaydip Sen[21]:** In the era of great technological advancement, we are living the dream of internet of Things, where are daily lives are assisted by smart technologies, gadgets enhancing peer to peer communication and productivity. The authors points that the IoT vision's greatest aspect is the significant

[21] Debasis Bandyopadhyay & Jaydip Sen, *Internet of Things: Applications and Challenges in Technology and Standardization*, 58 WIRELESS PERS COMMUN 49–69 (2011), http://link.springer.com/10.1007/s11277-011-0288-5 (last visited Oct 24, 2021).

impact it will have on various elements of everyday life and potential users' activities. The most noticeable effects of the IoT will be visible in both the working and domestic spheres from the perspective of a private user. Assisted living, smart homes and offices, e-health, and enhanced learning are just a few examples of potential application scenarios in which the new paradigm will play a pivotal in shaping the future. Similarly, the most prominent impacts will be equally noticeable from the standpoint of business users in domains like as automation and industrial manufacturing, logistics, business process management, and intelligent transportation of people and products. Further, the authors try to get our attention on the infancy of laws related to IoT, as legal norms regarding the impact of location on "Privacy" regulation, and the issue of data ownership in collaborative clouds of 'things' Network and data anonymity are yet to be framed or if framed, needs amendment.

15. **Alex B. Makulilo[22]:** Through her writing, the author highlights the fact that the development of "information and communication technology", combined with the innovation of the computer, Big Data, the Cloud, and the "Internet of Things" have recently fueled these concerns for "Privacy" because of the size and amount of data that can be collected, the speed at which such data can be collected, increased data storage capacities, especially in the Cloud, increased possibilities of manipulating our personal data, and the ease with which personal information can be shared across space and social media. "Privacy" is a contextual idea. What society views as private In society B, A might not be the same. People are not impacted in the same ways even though they share the same culture. People in wealthy nations—especially those in Western Europe—are more worried about "Privacy" than people in developing nations. In

[22] Alex B. Makulilo, *The Context of Data "Privacy" in Africa*, 33 *in* AFRICAN DATA "PRIVACY" LAWS 3–23 (Alex B. Makulilo ed., 2016), http://link.springer.com/10.1007/978-3-319-47317-8_1 (last visited Oct 24, 2021).

actuality, because of how strongly people in African civilization depend on one another, the concept of “Privacy” is very new. After colonial control ended in the 1960s and globalization began to impact Africa, “Privacy” came to be seen as a fundamental human right. But political unrest and strong executive leaders prevented citizens' rights from ever truly expanding. The journey for establishing basic rights was very challenging for African people. It was their sincere efforts and strong will which lead the victory for Citizens rights which cleared the path for adapting “AU Convention on Cyber security and Personal Data Protection” 2014. This act focused on three spheres, namely electronic transactions, personal “Data Protection” and cybercrimes. Although proper implementation still remains a challenge as these enactments hasn’t seen sunlight yet.

16. **Kriangsak Kittichaisaree[23]:** In comparison to the past, electronic devices and the Internet are comparatively inexpensive. Aside from being used for good, they can be prone to "digital abuse," such as being used for monitoring that invades a person's “Privacy”. With the enhancement of data providers, cloud storage and faster computing system, individuals are generating more user data than ever before. Tech giants are collecting these data under the cover of “better customer experience”. However, many a time it has happened that, they have failed to protect such data or provide any logical explanation against questions such as “where are the data being stored and what legislations are being applied on such storage facilities?”. The lacuna in data “Privacy” norms still exists in the 5th generation of internet and trends to get bigger, unless global

[23] Kriangsak Kittichaisaree, *Regulation of Cyberspace and Human Rights*, *in* PUBLIC INTERNATIONAL LAW OF CYBERSPACE 45–152 (Kriangsak Kittichaisaree ed., 2017), https://doi.org/10.1007/978-3-319-54657-5_3 (last visited Oct 24, 2021).

community doesn't come together and reinforce national and international "Data Protection" regime.

17. **Lee Andrew Bygrave[24]:** The authors argues for a uniform "Data Protection" regime where data "Privacy" agencies should be free from any kind of restriction to ensure their Independence. He further advocates for adopting new and effecting sensitization program to educate commoners regarding the importance of "Privacy" and their data, as without active participation of the 'users of technology' data security cannot be achieved. The author then turns to transnational cooperation and inter-legal aspects of data "Privacy" law, where he discusses on the need to 'information sharing' platforms to ensure check and balance in the system.

18. **Jeffrey Rosen[25]:** There is a gray area between the right to "Privacy" and the "Right to be forgotten". According to the author, the "Right to be forgotten" can be both a blessing and a curse in terms of the right to "Privacy" because it has two sides that affect both service providers and customers. As, the avenues are quite new the author suggests for further study in this area, while advocating for establishing a connecting link between "Right to be forgotten" and "Freedom of Speech", as it seems both of them may collide on a point.

[24] Lee Andrew Bygrave, Data "Privacy" Law: An International Perspective, 25 KING'S LAW JOURNAL 497–499 (2014), https://www.tandfonline.com/doi/full/10.5235/09615768.25.3.497 (last visited Oct 24, 2021).
[25] Jeffrey Rosen, *The "Right to be forgotten"*, 64 STAN. L. REV. ONLINE 88 (2011), https://heinonline.org/HOL/Page?handle=hein.journals/slro64&id=89&div=&collection=.

19. **Jef Ausloos[26]:** The 'default of forgetting' has gradually transitioned to a 'default of remembering' as new technologies have emerged. This has prompted many people to consider the concept of a "“Right to be forgotten”." The European Commission has recently demanded clarity on the idea and has attempted to define it on its own. The right, it could be argued, implies that the selected personal information must be permanently erased. When a person withdraws his or her consent or declares a desire to discontinue the processing of “personal data”, the data should be permanently erased from the data processor's computers, according to the author. To provide people control over their personal data, most nations rely on a consent regime. Individuals' 'power' to consent is typically regarded sufficient protection of “Privacy” in a free and democratic society. Practice, on the other hand, has exposed the flaws in this method. People don't read “Privacy” rules because they're written in legalese. Externalities in the network, lock-in, and a lack of viable alternatives frequently drive people to assent. Even if a person withdraws consent, that does not guarantee that his or her data will be erased retroactively. In a world of complexities ‘“Right to be forgotten”’ may give some control back to the owners of data.

20. **Anna Bunn[27]:** This author examines the much-discussed ‘“Right to be forgotten”' in light of the “European Court of Justice” (ECJ) judgement in the case of Google Spain SL, “Google Inc. v Agencia Espanola de Protecci on de Datos” (AEPD), Mario Costeja Gonzalez, issued in 2014. It also looks at the present EU “Data Protection” Directive's 'right of erasure,' as well as a suggestion that the new EU “Data Protection” framework incorporate a new right of erasure. The author correctly points out that we must first

[26] Jef Ausloos, *The ‘“Right to be forgotten”’ – Worth remembering?*, 28 COMPUTER LAW & SECURITY REVIEW 143–152 (2012), https://linkinghub.elsevier.com/retrieve/pii/S0267364912000246 (last visited Oct 24, 2021).
[27] Anna Bunn, *The curious case of the “Right to be forgotten”*, 31 COMPUTER LAW & SECURITY REVIEW 336–350 (2015), https://linkinghub.elsevier.com/retrieve/pii/S0267364915000606 (last visited Oct 24, 2021).

define the "“Right to be forgotten”," pointing out that the terms "right to oblivion" and "right to have your data erased from storage" can be readily misconstrued. According to the author's research, there have been some advancements in this murky area of the “right to Privacy”, but more clarification is required because the “Right to be forgotten” cannot rely solely on particular rulings. Since it's a worldwide phenomenon, attention must be paid to it globally.

Statement of Problem:

In the twenty-first century, data is considered to be the new fuel that is pumping the global economy. Today, data is transforming the macro to micro world businesses, entertainment industry, managing homes, and individual’s digital existence. It can further be used in a study to help cure a disease, increase a company's revenue, make a building more efficient and effective, or be the source of those annoying targeted adverts. In short, data is present everywhere. As the idea of the metaverse is realized, and the world we know is getting covered within the webs of the internet, the global population is getting the least concerned about their “Privacy”. The world literatures are ample, though not saturated, that focus on the issues of “Privacy” and data “Privacy” specifically in cyberspace while analyzing it with a constitutional perspective is missing, though the entire analysis has not been done as a whole in any single piece of work. A few researchers while exclusively investigating the various issues of “Privacy” and data “Privacy” protections and challenges of the same. After reading a number of research papers, policy documents, laws of many countries, international instruments, judgements, specifically of India Us and European Union. etc., the review of literature has been thematically organised in way and manner which this research aims to fulfil. In such a situation: The first issue is the task of defining what amounts to ‘“Privacy”’, ‘data “Privacy”’, and 'cyberspace’. “Privacy” is possibly the most challenging of all the human rights in the international inventory to define and limit. The concept of “Privacy” has

a long history, early Hebrew culture, Classical Greece, and ancient China all idolized the concept of “Privacy”, mostly focusing on the right to cloister. The global community has always defined the concept of “Privacy” according to the circumstances, for example in the Indian societal system one particular class of citizens were required to choose solitude at his last stage of life (Vanaprastha and Parivrajaka), whereas in African society the concept of solitude was considered to be a taboo, as in that society people were interdependent on each other for resources. So “Privacy” is defined in a variety of ways depending on the context and surroundings. The notion has been merged with “Data Protection” in many nations, which interprets “Privacy” in terms of personal information management. Outside of this relatively stringent setting, “Privacy” protection is commonly considered as a way of defining how far society can pry into a person's personal concerns. In this context, the problem, that is what amounts to “Privacy” and the ‘limit of Intrusion’ in one’s “Privacy” or ‘breach of private data in cyberspace’ remains un-answered. Further, we live in a society where data plays a crucial role in the day-to-day decision-making process, from multi billiondollar companies to network-service provider’s recharge packs, every single decision is backed by data. For instance, from waking up in the morning to going back to bed, a working person spends a considerable amount of time with his/her smart gadgets, in this process we, knowingly or unknowingly generate tons of data. This data is used for various commercial purposes. The problem which stands in such a situation is, ‘to what extent data can be used by a third party or shall the third party have certain limitations on collecting and using anyone’s data without his/her consent? This uncertainty poses challenges to resolve the issues of “Privacy” violations. The existing laws at national level lack any definition of data “Privacy” with proper 15 demarcation and extent of protection of an individual’s data against unscrupulous, uninformed access, misappropriation, and disclosure of personal data. With the development of science and technology individuals and associations are gaining more access to the private

spheres of one’s personhood. It will not be wrong to say that the avenues of “Privacy” are shrinking day by day. Recent issues like Pegasus spyware usage has shown that, even the preachers of democracy, having the intention to gain the political and strategic upper hand, can opt for using spyware to gain access to personal data belonging to influential personalities. The same can be true for other netizens of society. In a constitutional set up it is considered that all netizens enjoy certain ““fundamental right”s”, and the duty to protect such rights is bestowed upon the state. Among such rights, the “Right to Privacy” of personnel data in cyberspace is an emerging fundamental facet of Human rights and constitutional jurisprudence which the state cannot deny. If the state can adhere to this issue and acknowledge the difficulties related to ‘protection of “Privacy”’ robust dedicated legislation can be created, which can cover issues like identity theft, “Data Breach”, phishing, etc. An absence of such legislation at national level puts the country into the danger of an increased and uncontrolled criminal activities in cyberspace. Artificial intelligence is a type of "intelligent computing" in which computer programs can detect, reason, learn, act, and adapt in the same way that people can. It is "intelligent" in the sense that it mimics human cognition. It is "artificial" because it includes the processing of computational data rather than biological data. The exponential development in computer processing and storage, as well as massive banks of data that can be probed to extract information, are driving AI's rising power. Many science fiction forecasts from the past appear to pale in comparison to the computational capacity of machines and improvements in robotics. The capabilities of AI will grow faster than humans can fathom or prepare for, with quantum computing on the horizon. With the advanced algorithms Individuals can be identified, tracked, and monitored across various devices, whether they are at work, at home, or in public. This means that, even if your personal data is anonymized, an AI can de-anonymize it based on inferences from other devices once it becomes part of a huge data set. This muddles the line between personal

and non-personal data. Further AI's capabilities aren't just restricted to data collection. It can also be used to sort, score, classify, evaluate, and rank people using information as input. This is frequently done without the person's consent, and they frequently have little power to influence or question the conclusions of these tasks. This in fact is a serious threat towards data “Privacy”, and a gamble on Individual’s ““fundamental right”s”. State’s intervention to ensure data “Privacy” by establishing new dimensions and parameters of legal accountability for all kinds of national intermediaries, as well as international intermediaries having presence in India, is inevitable in the era of digitalization. International legislations like “UDHR (Art 12)” highlights that a person should not be deprived of his “right to Privacy”, and the state should adhere to the responsibility to implement the same through domestic policies. Similarly, the “International Covenant on Civil and Political 16 Rights (ICCPR)” also prohibits such interferences and attacks. India, being a democratic country became a signatory of these two covenants, acknowledging “Privacy” as a right. However, the ideology of “Privacy” didn’t find its place in the “fundamental right”section and was left for the judiciary to interpret the same under the purview of “Judicial activism”. As a result, the executive and the legislator had a small role to play to create legislation. In 2013, Edward Snowden, founder of WikiLeaks brought terabytes of data into the public domain, which clearly showed how public and private service providers can collect customer data and use them according to their whims and fancies. As we are residents of a technologically advanced era, it is evident that “Privacy” concerns are going to increase unless states take strict cognizance of these issues. The Internet remembers everything; this statement is true in its very sense. Whatever is uploaded in the world of the web, can never be actually taken down. This situation possesses a considerable amount of threat to the right to “Privacy”. The “Right to be forgotten” is a sine qua non of the “Right to Privacy”. In today’s world, gathering information regarding a particular individual is not a big challenge at all. It is noteworthy that

the data consumers are themselves the primary accomplice of their personal “Data Breach”. After the social media giants took over our public communication platform, we got used to a virtual world and shared our achievements, emotions, life events over our profile indiscriminately. It took a long time for us to understand that, once something is uploaded to the internet, it is likely to stay there. The twenty-first century is a world of surveillance cameras, phishing, and cyber-attack. It will be foolish to think that perpetrators will leave any chance to peep into someone’s private lives to gather some valuable data, which later can be encashed. In such a situation, ‘Right to be forgotten” or ‘Right to redeem personal data from the internet can find its place inside the directory of “fundamental right”. The “Right to be forgotten” is one of the novel dimensions of the right to “Privacy”; numerous European enactments have acknowledged this concept earlier. Many criminal convictions are thought to be "spent" after a specified period of time in the United Kingdom, specifically under the “Rehabilitation of Offenders Act”. This regulation suggests that after a person has served his jail term and has learned their lesson, he or she should have a right to lead a normal life again. To avoid such a situation European legislation while acknowledging the right to “Privacy” also acknowledged the “Right to erasure” or the “Right to be forgotten”. In recent times countries like India, through judicial interpretation have also acknowledged the same. On the contrary, the US constitution favours Transparency, the “right to free speech”, and the “right to know” over the “Right to be forgotten”. It is clear that a grey area exists where the “Right to be forgotten” and right to information are holding contradictory grounds.

Hypotheses:

In the absence of techno-legal regulation, the use of “Artificial Intelligence” (AI) and Unmonitored Data Collection system is leading to the violation of “Privacy” and the existing framework of “Data Protection” and “Privacy” is inadequate to handle the issues of “Privacy” & data “Privacy” in cyberspace.

Research Objectives:

1. To analyze the importance of acknowledging the right to "Privacy" in cyberspace as a "fundamental right".

2. To study the contours of a state regulatory regime defining the rights and liabilities of netizens and cyber world stakeholders including intermediaries.

3. To understand the need of establishing mandatory international minimum common standards to protect the right to "Privacy" in the cyber world, irrespective of territorial jurisdiction.

4. To analyze the complexities of Right to "Privacy" in an Artificial Intelligence (AI) led cyberspace.

5. To Study the concept of the "Right to be forgotten" and analyse the importance of the concept in context to the Right to "Privacy".

Research Question:

1. What are the attributes of the Right to "Privacy" as a basic feature of contemporary constitutionalism and whether these attributes extend to cyberspace?

2. Whether an international accountability mechanism is necessary for regulating intermediaries and stakeholders of cyberspace and cyber activities and what would be the role of States in such a mechanism?

3. What should be the contours of the mandatory international minimum common standards to protect the "right to Privacy" in the cyber world?

4. Whether personal information analysis by Artificial Intelligence (AI) can intrude inside the domain of "Privacy" violation in the realm of cyberspace?

5. Whether "Standard format e-contracts and e-consent" provisions, used in cyberspace, qualify the 'free prior informed consent' parameter in the context of data "Privacy"

Significance of the Study:

The utility of this study lies with the fact that even though data "Privacy" and the indispensability of "Data Protection" is emerging as a serious concern in India as well as around the globe; yet there are few comprehensive legislations in this regard, rather some rules and regulation has been made and a few regulations has been drafted which are also subjected to several lacunas. So in this study I will explore the different facets of data "Privacy" issues, "Data Protection", the international conventions addressing data "Privacy" and protection of personnel data in cyberspace, comparative analysis of various national "Data Protection" laws, and international "Data Protection" policies etc. The objective of the study is to figure out the adequate solution and suggest a model law.

Research Methodology:

I have adopted the doctrinal legal research method for achieving the objectives of this research. I have analyzed various primary sources such as the International laws like the "General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR)", "Privacy Act of 1974 of USA", "Personal Data Act of Finland", "Data Protection Act (Germany)" and National Legislations like "Information Technology Act 2000" "Digital Personal Data Protection Act 2023", "Indian Penal Code 1860", "Indian Evidence Act 1872" as well as Secondary data sources such as books, journals, articles, newspaper reports. As the Research stands in the socio-politico-legal as well as the technological domain, I have also focused on doctrinal methodologies as the primary method of research. Further, the research commands equal devotion in national as well as international instruments, policies, regional arrangements, and policies of mega-private stakeholders of the present domain i.e. cyberspace.

CHAPTER 2

Conceptual Framework of Right to "Privacy"

Introduction:

The ability to control one's personality is a prerequisite for the right to "Privacy". Its foundation is the notion that all people are born with certain inalienable rights.. Life's human component cannot be ignored. It is impossible to conceive without natural rights. The State does not grant natural rights. Because humans are human, they are inherently human. They are present in every person equally, regardless of gender, orientation, or social class. Dignity has usefulness both in and of itself. The constitution upholds human dignity as an innate value that is both a right and an interest[28].

Freedom and dignity are intrinsically related in their instrumental sense; one is a means to the other. Individual "Privacy" is a crucial component of dignity. The ability of a person to protect their private space allows for the attainment of the full value of life and liberty. A more expansive definition of liberty includes "Privacy" as a subset. Not every liberty can be used in private. Others, however, can only be satisfied in a private setting[29]. A person's body and mind can remain autonomous when they are in "Privacy". Autonomy is the ability to make decisions regarding significant life concerns on one's own. This essay will focus on the evolution of the concept of "Privacy" and how "Part III of the Indian Constitution" recognizes it as a basic right. Additionally, the paper will go over how India's technological advancements have affected the perception and implementation of the "right to Privacy"[30].

[28] Payal Thaorey, *LEGAL INTROSPECTION TOWARDS THE DEVELOPMENT OF RIGHT TO "PRIVACY" AS "FUNDAMENTAL RIGHT" IN INDIA*, 11 INDONESIA LAW REVIEW (2021).
[29] *Id.*
[30] *Id.*

“Right to Privacy” as basic feature of contemporary constitutionalism:

The “Privacy” debate essentially erupted in the twenty-first century with the necessity for data “Privacy” regulations and civil rights of “Privacy” for all individuals, regardless of sexual orientation. “Privacy” is a “fundamental right” protected by the “Constitution” and is essential to life and liberty. It exists in all people, regardless of class, socioeconomic status, gender, or sexual orientation. It is essential for the development of one's self, integrity, and dignity. However, because “Privacy” is not an absolute right, any invasion must be justified by law and must be founded on legality, need, and proportionality to protect this prized right[31]. In India, the right to “Privacy” is protected by the constitution even though it is not a separate basic right. Regretfully, the “right to Privacy” is not one of the "reasonable restrictions" to “The Freedom of Speech and expression” under “Article 19(1)(a)”. According to Article 19:

“Article 19” states that firstly The right to “Freedom of Speech” and expression belongs to every citizen; secondly, Nothing in sub-clause (a) of clause (1) shall impair the operation of any law already in effect or prohibit the State from enacting any law so long as the law imposes reasonable limitations on the exercise of the right granted by the said sub-clause in the interests of public order, decency or morality, defamation, incitement to commit an offense, friendly relations with foreign states, Indian sovereignty and integrity, security of the State, or any of these. Because the prohibitions have been carefully defined, a publication that intrudes on an individual's “Privacy” does not violate “Article 19(2)” unless it is "immoral" or "indecent." However, despite this gap, the courts have been able to creatively construe “the rights to life and freedom of movement” to carve out a basic right to “Privacy” The

[31] Kumar, Rahul, Jurisprudence of Right to “Privacy” in India (July 30, 2020). Available at SSRN: https://ssrn.com/abstract=3664257 or http://dx.doi.org/10.2139/ssrn.3664257 .

“fundamental rights” to life and liberty guaranteed by “Article 21” of the Constitution implicitly include the right to “Privacy”. In addition, the Indian judiciary has established the notion of “Privacy” as a component of the “right to life” through numerous rulings. For example, the question of how far the state can authorize surveillance is addressed in the cases of “*Kharak Singh v. State of U.P., Gobind v. State of M.P*” and “*Malak Singh v. State of P&H”* Rephrasing the question, it might be, to what extent can the state violate an individual's right to “Privacy” under the pretext of public safety? Court rulings have established that surveys can be carried out on those who have a criminal record or who could be a threat to public safety in general. A clear boundary separating the safety of individuals from that of criminals must exist. Since the devastating Snowden revelations in May 2013, governmental monitoring and citizens' right to “Privacy” have been at the centre of global debate due to advancements in science and technology. Reports about Indian bulk surveillance started to trickle in as the Snowden documents revealed, detail by detail, the extensive surveillance systems used by the American and British intelligence agencies (PRISM and TEMPORA, among others) to spy on both their own citizens and on communications elsewhereIt is now known that two systems exist in India and are in different stages of development: Netra, a dragnet surveillance system that finds and gathers electronic communication that uses specific keywords like "attack," "bomb," "blast," or "Kill," and Central Monitoring System (CMS), which allows the collection of telephone metadata by sifting through the records of telecommunications companies. The “right to Privacy” is a fundamental component of the “Indian Constitution”. According to numerous precedents set by Indian courts. In the age of the internet, this right requires more protection than ever.

Constitutionalism and a Study of Global Constitution:

Constitutionalism can be used both descriptively and prescriptively. This feature of the term was encapsulated by law professor Gerhard Casper, who observed, "Constitutionalism has

both descriptive and prescriptive connotations." When used in a descriptive sense, it mostly alludes to the historical fight for the people's right to "consent" and a number of other rights, freedoms, and privileges to be recognized by the constitution. When used prescriptively, its meaning encompasses the aspects of governance that are thought to be fundamental to the Constitution[32]. One of constitutionalism's most prominent features is that it defines the source and bounds of governmental power that is drawn from basic law. Constitutionalism "is the name given to the trust which men repose in the power of words engrossed on parchment to keep a government in order," as William H. Hamilton puts it, capturing this dual aspect[33]. Furthermore, discussions of the "concept of constitutionalism" always centre on the legitimacy of government, regardless of whether they have a descriptive or prescriptive focus. The concept of constitutionalism, for instance, helps to define what "grants and guides the legitimate exercise of government authority, "according to a recent evaluation of American constitutionalism[34]. If we consider the Indian aspect, we will find that All the persons who are occupying higher government posts and head of the states are to protect the Constitution and the People of India. Historian Gordon S. Wood claims that the constitution, which even controls the supreme authority of the state, was drafted using the most "advanced thinking" on the nature of constitutions[35].

Deciphering 'Privacy" as a Right:

The concept of the "right to Privacy" is incredibly fascinating. There are a minimum of three convincing arguments for why this concept is "intriguing." One, because of its "defused" nature, this right may be difficult to articulate even while it is easy to grasp or experience.

[32] Yash Kulshreshtha, *Overview: CONSTITUTIONALISM_THE SINE QUA NON OF A DEMOCRATIC SOCIETY*, YLCUBE, https://ylcube.com/c/blogs/overview-constitutionalism_the-sine-qua-non-democratic-society/ (last visited Feb 13, 2024).
[33] Gerhard Casper, *Constitutionalism*.
[34] Christian G. Fritz, *American Sovereigns: The People and America's Constitutional Tradition Before the Civil War (Prologue)*, (2008), https://papers.ssrn.com/abstract=1120409 (last visited Feb 13, 2024).
[35] Jeffery L. Johnson, *A Theory of the Nature and Value of "Privacy"*, 6 PUBLIC AFFAIRS QUARTERLY 271 (1992).

Second, while we declare that the constitution does not define this right, we subsequently learn that it is enshrined throughout Part III of the document in general and “Article 21” in particular. Stated differently, with a little introspective thought, what was initially invisible becomes apparent. Third, even though this right is very personal, we understand that it has no real significance for a person living alone; instead, it only has substance and meaning in the social context—in the company of "significant others"—while pleading for "let me be alone"! Whatever the case, the right to “Privacy” appears to have developed alongside social order; it predates even the concept of “Privacy”.

The word "privacatus," which meaning "separated from the rest of the world," is where the word “Privacy” first appeared. “The concept of Privacy” is incredibly intricate and challenging to understand. Due to its subjective nature, the term “Privacy”" has been interpreted differently depending on the context. According to Jude Cooley[36], who clarified the law governing “Privacy”, “Privacy” is synonymous with the right to be let alone." "Right to “Privacy” is bound to include body's inviolability and integrity and intimacy of personal identity including married “Privacy”, according to Tom Gaiety[37]. "Zero relationship between two or more persons in the sense that there is no interaction or communication between them, if they so choose" is how Edward Shills[38] defined “Privacy”. In very elegant words, Warren and Brandeis[39] have explained that "the idea of a private sphere is in which man may become and remain himself once a civilization has made distinction between the 'outer' and 'inner' man, between the life of the soul and the life the body." A neutral relationship between individuals or groups, or between individuals and groups, is what “Privacy” is. “Privacy” is a

[36] Thomas Cooley, *A Treatise on the Law of Torts or the Wrongs Which Arise Independent of Contract*, BOOKS (1879), https://repository.law.umich.edu/books/11.
[37] REDEFINING “PRIVACY” | Office of Justice Programs, https://www.ojp.gov/ncjrs/virtual-library/abstracts/redefining-”Privacy” (last visited Feb 13, 2024).
[38] Edward Shils, *“Privacy”: Its Constitution and Vicissitudes*, 31 LAW AND CONTEMPORARY PROBLEMS 281 (1966).
[39] warren-brandeis.pdf, https://www.cs.cornell.edu/%7eshmat/courses/cs5436/warren-brandeis.pdf (last visited Feb 13, 2024).

cultural concept, state, or value that varies from society to society and is aimed at the individual's collective self-realization. A prerequisite to the expansion and redemption of personhood is “Privacy”. "A recognition of one's ownership of his or her physical and mental reality and a moral right to his or her self-determination," according to Jeffrey Reiman[40], is what “Privacy” is all about. “Privacy” can be defined as an individual's sacred space or inviolable private area, but it is also influenced by their interactions with other members of society. Because these relationships invariably raise issues regarding an individual's autonomy and “freedom of choice”. Furthermore, societal features that compel a person to give up their autonomy are designed by the State and non-state actors[41].

The four characteristics of “Privacy” are “solicitation, intimacy, anonymity, and reserve” reflect the range of meanings associated with the term. "Solitude is a physical separation from others," claims Westin[42]. A close, easygoing, and honest relationship resulting from the seclusion of a pair or small group of people is called intimacy. It can involve two or more people. People's desire for moments of public “Privacy” is anonymity. Finally, reserve refers to the establishment of a psychological barrier that prevents unwanted intrusion; others must respect an individual's need or desire to limit the communication of information about them. “These qualities of Privacy” have made it into an inalienable right since they are essential to a person's existence. Right is "an interest and protected by a rule of right" according to Salmond[43]. It is any interest that one has an obligation to uphold and a wrong to ignore. According to Salmond's definition of a right, everyone has a right to “Privacy”, hence in addition to being recognized, it must also be protected from interference by the government

[40] Johnson, *supra* note 13.
[41] Right To “Privacy”, https://legalserviceindia.com/legal/article-7857-right-to-”Privacy”.html (last visited Feb 13, 2024).
[42] Leon A. Pastalan, *“Privacy” as a Behavioral Concept*, 45 SOCIAL SCIENCE 93 (1970).
[43] B. Patel, *Jurisprudence and Philosophy as Foundations of Law* (2001), https://www.semanticscholar.org/paper/Jurisprudence-and-philosophy-as-foundations-of-law-Patel/05f0783d35fa426ad024503e9e53e2072fefaec7 (last visited Feb 13, 2024).

and other parties. The right to “Privacy” consists of three parts. They are listed in the following order: First of all, The first feature of “Privacy” is physical or geographical “Privacy”, or more precisely, personal space. For instance, several types of “Privacy” are adequately relevant to the safeguarding of constitutional liberty. According to the second piece of content, the main “Privacy” concern is choice—the ability of an individual to make significant decisions without external interference. The third aspect of “Privacy” pertains to the safeguarding, maintenance, and exchange of personal data.

Understanding “Privacy” In the Light of Individualism:

In his article titled The Meanings of “Individualism” Steven Lukes[44] explains how the idea of “Privacy” has changed and developed as a result of how “Individualism” is perceived. Individualism is an ethical perspective that stresses "the moral worth of the individual" and can be found in political theories, ideologies, social perspectives, or ethical positions. A person is an independent entity since their creator gave them life, and as such, they are entitled to all freedoms, including “Privacy”, claims the individualism argument. According to the definition of “Privacy”, everyone has the right to enjoy their personal space, commonly referred to as the “right to solitude”. The concept is predicated on the autonomy of the person. The ability to make decisions is fundamental to human personality. A person's ability to assert and control their inherently human nature is derived from the concept of “Privacy”. The ability to make decisions about matters that are private and personal demonstrates the unbreakable nature of the human psyche. An individual's right to “Privacy” is associated with their sense of autonomy. When it comes to these matters, there is a “right to Privacy”. The human personality is comprised entirely of the mind and body. The preservation of a private space that allows for the development of an individual's personality is a “fundamental right” and preserves the integrity of the body and the sanctity of the mind. Thus, “Privacy” is

[44] Steven Lukes, "*The Meanings of Individualism”* 32 JOURNAL OF THE HISTORY OF IDEAS 45 (1971).

essential to human dignity. Every person is entitled to a private area where social norms have no influence over their ideas and actions. An individual is not subject to peer judgment in that zone. Individuals can make important decisions in “Privacy”, which discover a home in the human psyche. It gives each person the ability to make important choices that are reflected in their unique personalities. It allows people to resist the pressures of society to conform to certain norms by maintaining their own opinions, thoughts, expressions, ideas, ideologies, preferences, and choices. Establishing a private space is a fundamental acknowledgement of diversity and the individual's right to stand out from the crowd and pursue their own unique path. A person's right to “Privacy” shields her from the prying eyes of the public regarding matters that are private to her. Both the individual and the location are linked to “Privacy”. Since each person determines how best to exercise their liberty in private, “Privacy” is the cornerstone of all liberty. Individual “Privacy” and dignity are closely intertwined in a pattern that is woven throughout culture from a thread of diversity. The essence of human nature is embodied in “Privacy”, which acknowledges the autonomy of every person to decide on matters that are personal and intimate. However, it is imperative to recognize that people reside in communities and are employed in communities. Their social surroundings both shapes and is shaped by their personalities. he individual is not a loner. Individuals' lives are continuously impacted by relationships and behavioural patterns that affect society as a whole. In addition, a person's life is continuously influenced by the social and cultural norms they absorb from their community. The condition of flux, “which represents a constant evolution of individual personhood in the relationship with the rest of society”, is the inspiration behind setting apart a space of rest for the individual. People's lives as members of society give rise to a reasonable expectation of “Privacy”, which ensures that, although each person has a space reserved for private, their ability to live a free and independent life is limited by the rights of others to live in peace.

How "Privacy" Developed in India:

Indian communities were ruled by traditional Hindu law prior to European invasion, which brought the idea of "Privacy" into our legal system. It differed from Hindu law, which recognized and upheld the demands of "Privacy" in a variety of circumstances, both throughout the colonial era and after independence. The ancient legal system acknowledged the sacredness of the family and home, the independence of the community, and the consequences for violating these standards. Likewise, Islamic law acknowledges "Privacy" as an inalienable right, as does every school of Islamic jurisprudence.[45] During the British era, criminal law began to define an individual's province of "Privacy". Criminal laws protected persons, property, and dwelling buildings; in particular, the Criminal Procedural Code of 1890 made it unlawful to force a woman to remain unchaste. In addition to protecting people's person and property, the law of torts gave another layer of protection to individual interests in their reputation, warning that even the slightest contact by someone in a fit of passion could result in assault and be subject to damages claims. The right to reputation was exercised through the application of libel and slander legislation. Prior to India's independence, the "Swaraj Act of 1895" covered matters including the right to vote, equality and "Privacy rights", "Freedom of Speech", and punishment for certain crimes. However, the drafters of the Indian Constitution in 1948 favoured the American model, which included the Act of Rights and certain civil liberties and human rights in "part III of the Constitution", which deals with "fundamental rights". Before the current Constitution was adopted, citizens had no rights. India's legal concept of citizenship and enforceable rights were established by the 1950 Constitution. Protections against search and seizure were included to the "fundamental rights" part of the Constitution during its writing. "Dr. B.R. Ambedkar"

[45] "Privacy" Law in India: A Muddled Field - I — The Centre for Internet and Society, https://editors.cis-india.org/internet-governance/blog/the-hoot-bhairav-acharya-april-15-2014-"Privacy"-law-in-india-a-muddled-field-1 (last visited Feb 13, 2024).

believed that it would be good to include these provisions in the Constitution, even though he recognized that the "Code of Criminal Procedure" already provided them. As a result, even while the concept of the right to "Privacy" is not new in India, its implementation and acceptance have surely changed with time.

Debate over Right to "Privacy" in Pre-Constitutional Era:

The Indian parliament deliberated on the constitution for two years, 166 days, during the "Constitution Assembly Debate," before all assembly members approved it. During the debates over whether or not the right to "Privacy" should be included in the list of "fundamental rights", "Alladi Krishnaswamy Ayyar", a member of the Constituent parliament, and "Mr. B.N. Rau", an adviser to the parliament, disagreed. BN Rau asserts that a person's "right to Privacy" may make it more difficult for law enforcement to carry out investigations, which might have an effect on the investigation itself. [46]. However, according to Ayyar, granting people the right to "Privacy" and confidentiality in correspondence would have terrible effects for civil litigation, as papers are an essential part of the evidence. In the plenary sessions of the "Constituent Assembly", there were two separate attempts to amend the chapter on "fundamental right" to include rights to "Privacy" provisions. On April 30, 1947, "Somnath Lahiri" advocated that the right to "Privacy" in correspondence be acknowledged as a fundamental freedom. Nevertheless, his suggestion was not adopted. A year later, "Kazi Syed Karimuddin" proposed to add the right of the people to be free from arbitrary searches and seizures of their person, place of residence, documents, and possessions to "Article 20 (Draft Article 14) of the Constitution". The right to "Privacy" was not successfully included in the attempts to make the Constitution a "fundamental right". Even while the "Constituent Assembly" was not a seminar on the right to "Privacy" and its amplitude, the suggested inclusion (which was eventually deleted) was in two specific areas,

[46] Shils, *supra* note 16.

namely searches and seizures. Although a close reading of the Debates reveals that the Assembly only discussed whether there should be an express provision guaranteeing the right to “Privacy” in the limited context of "searches" and "secrecy" of correspondence, larger aspects of the right to “Privacy” were not fully explored during the debates. Whether or not the many aspects of the right to “Privacy” are included in the definition of "liberty" as stated in “Article 21” was not addressed[47]. It is not implied by this that the “Constituent Assembly” made a formal decision to deny the right to “Privacy” status as an essential part of the “freedoms and liberty” guaranteed by the “fundamental rights”. “Part III of the Constitution” does not have a particular clause on the right to “Privacy” since the assembly declined to adopt one.

Constitution vs. Constitutionalism in India:

“M.P. Sharma v. Satish Chandra”[48] marked the first instance in which “Privacy” was examined from a legal perspective. “The Criminal Procedure Code” grants the state the authority to issue search warrants, but the petitioner had contested this authority. "The provision declaring that the state has an overriding power in law for affecting search and seizure is for the purpose of security," the Court ruled in this case. Furthermore, the “Chief Justice Mehr Chand Mahajan”-led Eight-Judge Supreme Court ruled, "We have no justification to import it, into a totally different “fundamental right”, by some process of strained constitution," Because the founders of the Constitution recognized a basic right to “Privacy”, akin to the “American Fourth Amendment”, they thought proper to exempt such control from constitutional limitations. In this evolving argument over “Privacy”, the court

[47] “B. SHIVA RAO, THE FRAMING OF INDIA’S CONSTITUTION A STUDY (1968)", http://archive.org/details/in.ernet.dli.2015.275967 (last visited Feb 13, 2024).
[48] M. P. Sharma And Others vs Satish Chandra, District ... on 15 March, 1954, https://indiankanoon.org/doc/1306519/ (last visited Feb 14, 2024).

has offered a highly conservative interpretation of the right to “Privacy”, holding that the authors of the Constitution did not include it and that the court should not compel it to do so.

Later, the Supreme Court addressed the issue of "whether surveillance under Chapter XX of the Uttar Pradesh Police Regulations 236(b) which allowed surveillance domiciliary visits at night was held to contravene Article 21" in “State of U.P. v. Kharak Singh”. A six-judge Supreme Court heard the matter. The court determined that the Constitution's preamble, which guarantees each person's dignity, upholds human ideals to ensure each person's full development and evolution. This makes the individual's personal liberty significant. We are referring to these framers' intentions only to highlight key ideas within the text of the Constitution, such as the necessity for words like "personal liberty" to be interpreted reasonably to fulfil their intended purposes. This does not entail interpreting the phrase in a way that is inconsistent with any dogmatic constitutional theories or preconceived notions. In an effort to give the term "personal liberty" a deeper meaning, the Court cited Frank further J., who noted in “Wolf v. Colorado”[49] that "the security of one's “Privacy” against arbitrary intrusion by the police is basic to a free society," with approval. Because of this, it is implied in "the concept of ordered liberty" and, as such, is protected by the Due Process Clause against the states. The knock at the door, day or night, as a pretext for a search based only on police authority and without legal authority is, in Murphy, J.'s words, an invasion that goes against "the very essence of a scheme of ordered liberty." It is clear from this ruling that the court began to recognize the need to protect “Privacy”, but this recognition is restricted to police actions that are not protected by the legally established due process. Furthermore, it can be argued that while “Privacy” protection will come later, “Privacy” recognition is crucial before protection. Even though the court did not clarify whether or not “Privacy” was recognized in this case, it did offer insight into how to protect it.

[49] “Wolf v. Colorado :: 338 U.S. 25 (1949) :: Justia US Supreme Court Center", https://supreme.justia.com/cases/federal/us/338/25/ (last visited Feb 14, 2024).

"Gobind v. State of Madhya Pradesh"[50] is an additional noteworthy case in which the Supreme Court conducted a more thorough examination of the right to "Privacy". The "Madhya Pradesh Police Regulations 855 and 856", allow for surveillance by several methods, including picketing and domiciliary visits to habitual offenders. The court was debating whether or not these regulations were constitutional. In this instance, the regulations passed the test of being a "procedure established by law," as specified in "Article 21", and the Supreme Court upheld their validity. A restricted right to "Privacy" based on "Articles 19(1) (a)35 (d)36" and "Article 21" was also recognized by the Court. Nonetheless, the Court did not believe that the right was unqualified. The Court held that, in accordance with "Article 19(5)", limitations on the right may be lawfully imposed in the public interest. Matthew J. anticipated that the "Privacy" right would develop on a case-by-case basis. The Court preferred to consider the factual circumstances of each case when making decisions regarding these claims.

The Court's decision was as follows: the right to "Privacy" will always require a case-by-case developing procedure. Therefore, even though we recognize that the right to "Privacy" is an outgrowth of "The Freedom of Speech", the right to personal liberty, and the ability to travel freely within India, we do not think that it is an absolute. As a result, we view the right to "Privacy" as essential.

It needs to be subject to restrictions based on a compelling public interest. Nevertheless, the compelling State Interest Test must be passed by the legislation that contravenes it. Consequently, the "Gobind Case" decision recognizes that to further the public interest or the larger welfare of society, some restrictions on the right to private may be required. The Supreme Court further recognizes that the basis for this kind of restriction need to be the

[50] Gobind vs State Of Madhya Pradesh And Anr. on 18 March, 1975, https://indiankanoon.org/doc/845196/ (last visited Feb 14, 2024).

compelling State Interest Test. In this case, Matthew J. has acknowledged that article 19's restrictions do apply and that the right to “Privacy” is recognized in specific circumstances. It is important to remember that determining what rights are restricted essentially amounts to accepting those rights. Without first acknowledging a right, we cannot restrict it. Consequently, the “Gobind case” revealed that although the court recognized the right to “Privacy” as a component of “articles 19(1)” and “Article 21”, it remained susceptible to restrictions imposed by the government on the basis of the government's interest and legally authorized acts. Furthermore, the scope of the right to “Privacy” can be construed differently based on the situation because there are no universally accepted norms for “Privacy”. In “R.M. Malkani v. State of Maharashtra”, the Supreme Court said that "the court will not tolerate safe guards for the protection of the citizen to be imperilled by permitting the police to proceed by unlawful or irregular methods"[51]. Therefore, the court declares that it will never, under any circumstances, allow any authority to infringe upon a person's right to “Privacy” other than through the proper channels set forth by law. The right to “Privacy” claim aids in deciding how and to what extent information about an individual, group, or organization will be shared with others. Whichever medium is used to store, preserve, or accumulate it doesn't matter. In essence, “Privacy” rights give people the assurance that the state cannot compel them to divulge any information that is gathered outside the bounds of constitutional validity. In the case of “Ram Jethmalani and Ors. v Union of India (UOI)” and Ors., the Supreme Court held that the right to “Privacy” is a fundamental constitutional principle and that the right to life is dependent upon it. People must have private spaces that are hidden from inquisitive eyes, unless they are involved in criminal conduct. The state cannot force citizens to provide information about them or make any information about them public unless it has done so through legally authorized investigations that fall within the four

[51]“ R. M. Malkani vs State Of Maharashtra" on 22 September, 1972, https://indiankanoon.org/doc/1179783/ (last visited Feb 14, 2024).

parameters of constitutional permissibility to receive benefits from the state or to assist in the investigation and prosecution of such individuals.

Therefore, unless the state establishes legitimate grounds for such disclosures, it cannot force an individual to disclose information if he does not wish to disclose, reveal, or submit it. A person's right to “Privacy” would undoubtedly be violated by coerced information disclosure. In this case, the court defined the boundaries of the right to “Privacy”, declaring that even the state cannot compel someone to give up their “Privacy” in the absence of a legal obligation. The right to “Privacy” and “The “Freedom of Speech”” and expression guaranteed by “Article 19 (1) (a) of the Indian Constitution” are in constant conflict. A citizen must take great care when using “article 19 (1) (a)” to express their thoughts, disagreements, opinions, experiences, etc. about other people to make sure that their use of the right does not lead to speech or other expressions about other people that could ultimately violate their right to “Privacy”. The Court in “R. Rajagopal v. State of Tamil Nadu” made several recommendations that might be used as the foundation for defining “Privacy” in an effort to find a middle ground between the interests of freedom of expression and the right to private. Here are some of the guiding ideas:

The right to “Privacy” is inadvertently included in a citizen's Article 21 rights to life and liberty. Every citizen is entitled to the protection of their personal data, including information on their marriage, family, procreation, motherhood, upbringing, and education. Nothing concerning the aforementioned subjects, positive or negative, factual or not, may be published without his consent. This is an infringement on someone's right to “Privacy”, and there could be legal ramifications. However, if someone voluntarily enters a debate, starts one, or brings it up, their viewpoint may differ[52].

[52] *Id.*

This is the most concise explanation of how “Article 21” protects the “fundamental right” to “Privacy”. Moreover, the law in this particular canon makes it clear that a claim for damages for breach of “Privacy” is permissible. Put otherwise, the invasion of “Privacy” may give rise to a civil lawsuit. Consequently, the “Auto Shankar Case” ruling establishes remedies for “Privacy” breaches in both public and private law[53]. Since the right to “Privacy” guaranteed by “article 21” of one citizen is evaluated in relation to another “fundamental right” granted under “article 19 (1) (a)”, namely “The “Freedom of Speech”” and expression of another citizen, this shows an interesting evolution regarding the nature of the right to “Privacy”. In this instance, the court looked at how a conflict between two individuals' “fundamental right”leads to the commercialization of a person's right to private.

Additionally, the right to “Privacy” is shielded from an individual. The principle that "a third party intrusion into one's “Privacy” results in grave violation of one's right to “Privacy” and hence implies need of legal protection to right to “Privacy” was upheld by Knight Bruce in the “Prince Albert v. Strange case”. When people violate each other's “fundamental right” to “Privacy”, it is detrimental to social order. As a result, the right to “Privacy” is shielded from both the government and private parties, including individuals. "“fundamental right” protect individuals from any arbitrary actions taken by both, the state as well as any individual," the court held in “Bodhisattwa Gautam v. Subhra Chakraborty”[54]. The right to “Privacy” requires that the state refrain from interfering in an individual's affairs and that other people refrain from doing the same. When someone interferes with another's right to “Privacy”, the state may take the appropriate action against them. Additionally, the scope of the right to “Privacy” has been broadened in this instance because a case-based evaluation will be

[53] Prince Albert v Strange (1849) 47 ER 1302 | Student Law Notes - Online Case Studies, Legal Resources and Audio Summaries, https://www.studentlawnotes.com/prince-albert-v-strange-1849-47-er-1302 (last visited Feb 14, 2024).
[54] Shri Bodhisattwa Gautam vs Miss Subhra Chakraborty on 15 December, 1995, https://indiankanoon.org/doc/642436/ (last visited Feb 14, 2024).

conducted in the event that a citizen's right to “Privacy” conflicts with that of another citizen. Therefore, protection is needed not only when two “fundamental right” collide, but also when one “fundamental right” the right to “Privacy” as guaranteed by “Article 21” of the Constitution confers with another.

Privacy as a Right on Global Platform:

USA’s Stand on Right to “Privacy”:

There is no explicit right to “Privacy” in the United States Constitution. But James Madison and the other framers of the Act of Rights expressed concern about certain aspects of “Privacy”, which are protected by the Act of Rights: the First Amendment's “Privacy” of beliefs; the Third Amendment's “Privacy” of the home against demands that it be used to house soldiers; the Fourth Amendment's “Privacy” of the person and possessions against unreasonable searches; and the Fifth Amendment's privilege against self-incrimination, which safeguards the “Privacy” of personal information. Furthermore, as stated in the Ninth Amendment, the Act of Rights' "enumeration of certain rights" "shall not be construed to deny or disparage other rights retained by the people." Although the meaning of the Ninth Amendment is unclear, some people have interpreted it as permission to read the Act of Rights broadly to protect “Privacy” in ways that are not expressly stated in the first eight amendments. Justice Goldberg was among those who held this opinion in his Griswold concurrence. Although the meaning of the “Ninth Amendment” is unclear, some people have interpreted it as permission to read the Act of Rights broadly to protect “Privacy” in ways that are not expressly stated in the first eight amendments. Justice Goldberg was among those who held this opinion in his Griswold concurrence. But starting in 1923 and continuing with more recent rulings, the Supreme Court has interpreted the Fourteenth Amendment's "liberty" guarantee broadly to protect a fairly broad right to “Privacy” that now includes choices

regarding raising children, having children, getting married, and stopping medical treatment. Most Americans, according to polls, are in favour of this expansive interpretation of the Constitution.

In two rulings from the 1920s, the Apex Court interpreted the liberty clause of the "14th Amendment" to forbid states from meddling in the private decisions made by parents and teachers regarding their children's education. In the 1923 case of "Meyer v. Nebraska"[55], the Supreme Court overturned a state statute that forbade teaching German and other foreign languages to students prior to their ninth grade. According to the state, teaching foreign languages to students could cause them to acquire "ideas and sentiments foreign to the best interests of this country." But in a 7–2 ruling authored by Justice McReynolds, the Court opined that the state had not demonstrated a compelling need to interfere with parents' and educators' rights to determine what curriculum is best for young pupils. In this case Justice McReynolds[56] reiterated that:

Although this court hasn't made an exact attempt to define the liberty thus guaranteed, the term has been given careful thought, and some of the things included in it have been stated unequivocally. It certainly refers not only to the absence of physical constraints but also to the "freedom to enter into contracts", to work in any of the common vocations, to learn useful skills, to get married, to start a family, and raise children, to worship God in accordance with his own conscience, and generally to enjoy those rights that have long been acknowledged by common law as necessary for free men to pursue happiness in an orderly manner.

Following that, the Court applied the Meyer principles in the well-known "Pierce v. Society of Sisters case" of 1925 to invalidate an Oregon statute that would have required all students

[55] Meyer v Nebraska (1923), http://law2.umkc.edu/faculty/projects/ftrials/conlaw/Meyer%20v%20Nebraska%20%281923%29.html (last visited Feb 14, 2024).
[56] *Id.*

to attend public schools, closing all private institutions in the state. The Warren Court of the 1960s gave new life to the "Privacy" doctrine of the 1920s when it overturned a state statute that forbade married couples from possessing, selling, or giving away contraceptives in "Griswold v. Connecticut"[57] (1965). Various explanations were put forth for the decision's outcome. Justice Douglas' opinion on behalf of the Court saw the "penumbras" and "emanations" of various Act of Rights guarantees as creating "a zone of "Privacy"," Justice Goldberg partially relied on the Ninth Amendment's reference to "other rights retained by the people," and Justice Harlan's decision maintained that the Fourteenth Amendment's liberty clause prohibited the state from engaging in actions that were incompatible with a government that was founded "on the concept of ordered liberty[58]."

The Court unanimously decided in 1969 that a person's right to own and watch pornography in his own home—including pornography that could serve as the basis for a criminal prosecution against its distributor or manufacturer—was protected by the right to "Privacy". "Whatever the justifications for other statutes regulating obscenity, we do not think they reach into the "Privacy" of one's own home," Justice Marshall wrote in "Stanley v. Georgia"[59], drawing support for the Court's ruling from both the 1st and 4th Amendments. If the First Amendment is any indication, it states that a State has no right to dictate to a man who is sitting by himself in his own home what kind of literature or movies he can watch or read.

Further In "Roe v. Wade" (1972)[60], the Burger Court expanded the right to "Privacy" to include a woman's right to an abortion. However, the court declined multiple requests to

[57] Griswold v. Connecticut, 381 U.S. 479 (1965), JUSTIA LAW, https://supreme.justia.com/cases/federal/us/381/479/ (last visited Feb 14, 2024).
[58] *Id.*
[59] Stanley v. Georgia, 394 U.S. 557 (1969), JUSTIA LAW, https://supreme.justia.com/cases/federal/us/394/557/ (last visited Feb 14, 2024).
[60] Roe v. Wade | Summary, Origins, Right to "Privacy", & Overturning | Britannica, (2024), https://www.britannica.com/event/Roe-v-Wade (last visited Feb 14, 2024).

further expand this right. The case of “Kelley v. Johnson” (1976)[61], in which the Court maintained a grooming policy for law enforcement personnel, exemplifies the movement to restrict the extent of the "zone of “Privacy”." (The Court did not address, however, whether the general public could be subject to a grooming law because it believed that people would have a right to “Privacy” regarding their appearance.) However, some state courts were not averse to expanding the boundaries of the private sphere. Of all the states, Alaska's Supreme Court went the furthest in defending individuals' right to “Privacy”. The Alaska Supreme Court determined that a citizen's right to possess and use small amounts of marijuana in his own home is protected by the constitution in “Ravin v. State” (1975)[62], citing precedents like Stanley and Griswold as well as the more expansive “Privacy” protections found in the Alaska Constitution. "The Constitution protects the sanctity of the family precisely because the institution of the family is deeply rooted in the Nation's history and tradition," the Supreme Court declared in the 1977 case of “Moore v. East Cleveland”[63]. Moore overturned a housing ordinance that forbade a grandmother from sharing a home with her two grandsons, finding “Privacy” protection for the decision of an extended family to live apart. Judge Powell stated in a court opinion that "the choice of relatives in this degree of kinship to live together may not be lightly denied by the state."

The right to choose whether or not to receive life-prolonging medical treatment is one of the liberties that people have in more recent decades, as the Court acknowledged in “Cruzan v. Missouri Department of Health” (1990)[64]. However, the Court acknowledged that states may place restrictions on the exercise of this right. In 2003, the Supreme Court overturned a

[61] Kelley v. Johnson, 425 U.S. 238 (1976), JUSTIA LAW, https://supreme.justia.com/cases/federal/us/425/238/ (last visited Feb 14, 2024).
[62] Ravin v. State, JUSTIA LAW (2024), https://law.justia.com/cases/alaska/supreme-court/1975/2135-1.html (last visited Feb 14, 2024).
[63] Moore v. City of East Cleveland, OYEZ, https://www.oyez.org/cases/1976/75-6289 (last visited Feb 14, 2024).
[64] Cruzan v. Director, Missouri Dep’t of Health, 497 U.S. 261 (1990), JUSTIA LAW, https://supreme.justia.com/cases/federal/us/497/261/ (last visited Feb 14, 2024).

previous ruling in “Lawrence v. Texas”[65], holding that Texas had violated the liberty clauses of two gay men by enforcing a state law that forbade homosexual sodomy against them. While deciding this case Justice Kennedy in his own words have stated that "These matters, involving the most intimate and personal choices a person may make in a lifetime, choices central to personal dignity and autonomy, are central to the liberty protected by the Fourteenth Amendment. At the heart of liberty is the right to define one’s own concept of existence, of meaning, of the universe, and of the mystery of human life....The petitioners are entitled to respect for their private lives. The State cannot demean their existence or control their destiny by making their private sexual conduct a crime. Their right to liberty under the Due Process Clause gives them the full right to engage in their conduct without intervention of the government. 'It is a promise of the Constitution that there is a realm of personal liberty which the government may not enter."[66] Through its “Privacy” rulings, the Court has grappled with the issue of how strong an interest a state must prove to win over citizens' claims that their rights to “Privacy” have been violated. Although later cases like Cruzan and Lawrence have indicated that the burden on states may not be as great as previously thought, earlier rulings like “Griswold and Roe”[67] suggested that states must demonstrate a compelling interest and narrowly tailored means when they have burdened fundamental “Privacy” rights.

Upon Considering all the case laws and precedents we can reach to a understanding that the US Judiciary is divided into two separate teams when it comes to protecting “Privacy” under the constitution. As the US Constitution does not have any specific or dedicated section acknowledging “Privacy” as a right, therefore the Right to “Privacy” many fold challenges in

[65] Lawrence v. Texas, 539 U.S. 558 (2003), JUSTIA LAW, https://supreme.justia.com/cases/federal/us/539/558/ (last visited Feb 14, 2024).
[66] *Id.*
[67] William Van Alstyne, *Closing the Circle of Constitutional Review from Griswold v. Connecticut to Roe v. Wade: An Outline of a Decision Merely Overruling Roe*, 1989 DUKE LAW JOURNAL 1677 (1989).

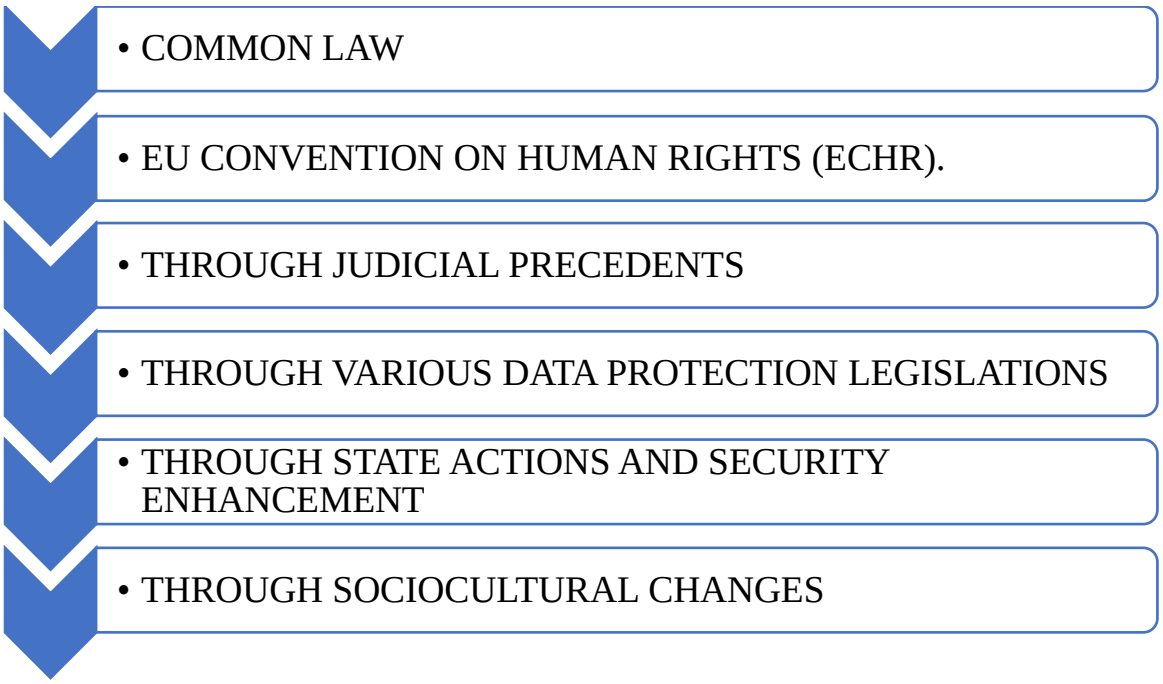
the Country. However with the assistance from Judicial activism the '"Privacy"' as a right has found it's place in the constitution.

Right to "Privacy" in UK- Yesterday, Today and Tomorrow.

Britain being the labour room of many modern day legislation, has surprisingly kept their inventory when it came to protecting '"Privacy"' as a right. The English common law does not expressly recognize a "right to "Privacy"." The Court in Wainwright v. Home Office[68] determined that there is "a great difference between identifying "Privacy" as a principle of law in itself and "Privacy" as a value which underlies the existence of a rule of law (and may point the direction in which the law should develop)." The idea of underlying values, or principles in the widest sense, that guide the development of English common law is well-known. It came to the conclusion that only the underlying value of "Privacy" exists, not the principle of the right to "Privacy". It can be said that the United Kingdom's conception of the right to "Privacy" has emerged from a blend of statutory law, common law principles, and changing social norms. Although the Fourth Amendment of the US Constitution is a single codified document that protects "Privacy", the UK does not have a similar document. However, a number of legal developments have helped to recognize and uphold the right to "Privacy".

How "Privacy" Developed in UK:

[68] House of Lords - Wainwright and another (Appellants) v. Home Office (Respondents), https://publications.parliament.uk/pa/ld200203/ldjudgmt/jd031016/wain-1.htm (last visited Feb 14, 2024).



Common law: There has been always a debate regarding whether "Privacy" is a common law or Human Right. The idea of "Privacy" has long been acknowledged by English common law, if somewhat implicitly. Over time, the courts have come to recognize concepts like the right to "Privacy" and the defense against unauthorized access to one's personal information. The concept of "Privacy" as a common law principle states that rather than using specific statute laws to protect private rights, courts should interpret and apply legal principles. Rather than through legislative enactments, common law develops through court decisions and precedents established in cases. "Privacy" rights have long been acknowledged and safeguarded by common law principles in numerous legal systems, including those that draw inspiration from the English common law tradition[69]. These principles may include the freedom from unjustified interference in one's personal life, the right to confidentiality in some communications, and safeguards against arbitrary searches and seizures. The common

[69] Michael Tilbury, *"Privacy": Common Law or Human Right?, in* EMERGING CHALLENGES IN "PRIVACY" LAW: COMPARATIVE PERSPECTIVES 157 (David Lindsay et al. eds., 2014), https://www.cambridge.org/core/books/emerging-challenges-in-"Privacy"-law/"Privacy"-common-law-or-human-right/3537CF826420DD4C1BA32188A0944625 (last visited Feb 14, 2024).

law principle of "Privacy"' adaptability to shifting social norms and technological developments is one of its advantages. Courts can interpret and apply common law principles to meet new "Privacy" incursions and growing challenges even in the absence of specific legislation. But there might be drawbacks to basing "Privacy" protection entirely on common law principles. Common law has a propensity to develop slowly, so it might not always keep up with the quick changes in technology or the shifting expectations of society with regard to "Privacy"[70]. Because of this, a number of jurisdictions have added statutory laws that expressly address "Privacy" rights in a variety of contexts, including "Data Protection", electronic communications, and consumer "Privacy", to the common law protections[71].

EUROPEAN CONVENTION ON HUMAN RIGHTS:

Ensuring the "Privacy" and family life of an individual is safeguarded by Article 8 of the European Convention on Human Rights, to which the United Kingdom is a signatory. "The Human Rights Act of 1998", which incorporated the European Convention into UK law, has had a major influence on the legal system's recognition of "Privacy" rights in the UK. "Article 8"[72] states that everyone is entitled to the respect of his or her home, family, and correspondence. No public authority may interfere with the exercise of this right in any way other than that which is permitted by law, necessary in a democratic society to protect the nation's economic security, public safety, or national security, to prevent disorder or crime, to protect one's own health or morals, or to defend the rights and freedoms of others. The "European Convention on Human Rights (ECHR)" is made enforceable within the UK legal system by the "Human Rights Act 1998", which was passed in the UK. Therefore, in situations where public authorities violate an individual's "Privacy", people in the UK can

[70] Van Alstyne, *supra* note 53.
[71] "Privacy" in English law, WIKIPEDIA (2023), https://en.wikipedia.org/w/index.php?title="Privacy"_in_English_law&oldid=1191895814 (last visited Feb 14, 2024).
[72] *Id.*

depend on the protections provided by Article 8 of the ECHR. The European Court of Human Rights (ECtHR) has interpreted the right to "Privacy" under Article 8 broadly to cover a variety of private life aspects, such as personal autonomy, personal "Data Protection", and communication confidentiality. In situations where it determined that the UK government had violated Article 8, such as when mass surveillance programs or improper use of personal data were involved, the ECHR has rendered rulings against the government of the UK.

DEVELOPING 'RIGHT TO PRIVACY" THROUGH JUDICIAL PRECEDENTS:

UK has a long history of Judicial Precedents through which UK has acknowledged 'Right to "Privacy"'. Let us have a quick look at them.

- Actors Michael Douglas and Catherine Zeta-Jones sued Hello! magazine in "Douglas v. Hello"! Ltd. (2000)[73] over the publication of unlicensed wedding photos. The court's ruling in their favour allows for the commercial exploitation of private gatherings without compromising the right to "Privacy".
- The supermodel Naomi Campbell sued Mirror Group Newspapers in "Campbell v. MGN Ltd" (2004)[74], alleging "Privacy" breach after the publication of information about her attendance at Narcotics Anonymous. Her case was heard by the House of Lords, which set a precedent for the UK's protection of private rights.
- Prince Charles sued the publishers of the Mail on Sunday in HRH "Prince of Wales v. Associated Newspapers Limited" (2006)[75], claiming that they had violated his "Privacy" by publishing passages from his personal journals. The Court of Appeal's

[73] Nicole Moreham, *Douglas and Others v Hello! Ltd. The Protection of "Privacy" in English Private Law*, 64 THE MODERN LAW REVIEW 767 (2001).
[74] House of Lords - Campbell (Apellant) v. MGN Limited (Respondents), https://publications.parliament.uk/pa/ld200304/ldjudgmt/jd040506/campbe-1.htm (last visited Feb 14, 2024).
[75] HRH The Prince of Wales v Associated Newspapers (No.3) (CA), 5RB BARRISTERS, https://www.5rb.com/case/hrh-the-prince-of-wales-v-associated-newspapers-no-3-ca/ (last visited Feb 14, 2024).

decision in his favor underscores how crucial it is to protect the confidentiality of private diaries.

- The former president of the Fédération Internationale de l'Automobile (FIA), Max Mosley, successfully sued News of the World for breach of "Privacy" in "Max Mosley v. News Group Newspapers Ltd". (2008)[76] after the newspaper revealed information about his participation in a private sadomasochistic sex session. Mosley was given damages by the court after it was determined that there was no public interest in the story.
- In "Vidal-Hall v. Google Inc". (2015)[77] In this case, Google was sued by multiple plaintiffs alleging "Privacy" violations stemming from tracking cookies utilized by Google's Double Click advertising network. The Court of Appeal set a major precedent in "Privacy" law when it decided that misuse of personal data could cause damages even in the absence of monetary loss.

  These cases paved way for British legislators to prepare a competitive guidelines for adhering with existing laws to protect their citizens right to "Privacy".

THROUGH REVISION VARIOUS "DATA PROTECTION" LEGISLATIONS

The UK has enacted several "Data Protection" regulations in the digital age to safeguard individuals' right to "Privacy". People have rights over how their personal information is used, and the "Data Protection Act of 2018" (which enforces the General "Data Protection" Regulation, or GDPR) of the European Union) and the "Data Protection" Act of 1998 both regulate the processing of personal data.

[76] Mosley v News Group Newspapers Ltd (No 3), 5RB BARRISTERS, https://www.5rb.com/case/mosley-v-news-group-newspapers-ltd-no-3/ (last visited Feb 14, 2024).
[77] Vidal-Hall v Google goes to the Supreme Court, CARTER-RUCK, https://www.carter-ruck.com/blog/vidal-hall-v-google-goes-to-the-supreme-court/ (last visited Feb 14, 2024).

THROUGH STATE ACTIONS AND SECURITY ENHANCEMENT

In the UK, there have also been legal discussions and disputes about the authority to monitor and investigate, especially in light of recent technological developments. The compatibility of the “Regulation of Investigatory Powers Act” 2000 (RIPA) and later laws with respect to “Privacy” rights has been questioned.

Social and Cultural Shifts

The evolution of “Privacy” rights in the “United Kingdom” has been subject to the influence of evolving cultural norms and social attitudes. Because social media is so widely used and because people are becoming more conscious of “Privacy”-related issues, they are learning how crucial it is to preserve their “Privacy” in all facets of their lives. All things considered, a range of legislative actions, court decisions, international agreements, and cultural changes have altered the UK's right to “Privacy”. The ongoing balancing act between people's rights and the legitimate interests of the state and society is reflected in this evolution.

Upon perusing the development of Right to “Privacy” throughout asian, American and European continents I am of the considered opinion that, at the very first day of any constitution no country has recognized “Privacy” as a “fundamental right” or a Right. No one has seriously taken this issue until their “Privacy” was someway violated. However, with the invention of new technologies maintaining our lives became more challenging and we did felt the requirement to have proper safeguards for protecting our “Privacy”. These concerns are addressed in the three sections.

Conclusion:

It is an exciting adventure to establish the “right to Privacy” as a basic right. It's an interesting development that the right to “Privacy”, which was once completely disregarded and ignored before the independence era, is now being recognized as a “fundamental right” with various facets and elements. Since the adoption of our constitution, members of the legislative and judicial branches have demonstrated a thorough and broad approach to recognizing, defending, regulating, and preserving the right to “Privacy” as an essential component of a democratic state through a number of laws and rulings. In harmony with India's constitution, “Privacy” has grown and changed in both horizontal and vertical dimensions. Horizontally, or within a person, it has encompassed sexual autonomy is a component of “Privacy”, but it also places vertical (state and individual) obligations on the state to uphold and preserve each citizen's right to “Privacy”. Based on the foregoing discussion, it is evident that the right to “Privacy” is a necessary component of the freedoms guaranteed by Articles 19 and 21 of the Constitution, as well as the rights to life and personal liberty. ”Privacy” rights are well suited to the advancements in technology, and their creation and preservation are unaffected by the media—online, print, or otherwise. The latest developments surrounding the “DPDP Act” mark a constructive step towards protecting the “right to Privacy” in the digital era, even though the regulations are still in the early stages and their exact implications remain unknown. The right to “Privacy” of the citizen must always come first.

I have mentioned earlier that we are all sworn to protect the constitution which protects us from any kind of state atrocities. This particular sentence has a deeper meaning. If we analyze it further we can understand that, As the ‘Right to “Privacy”’ protect us from anykind of State Intrusion, we also have the responsibility to protect this right from any kind of unwanted changes. We also have the responsibility to upgrade this right with better features, so that it can survive the critical test of time. None the less, I would like to conclude this Chapter by

saying that ‘Right to “Privacy”’ is a part of contemporary constitutionalism and it shall continue to be a part of a country’s constitution, so that it can protect the original decision makers of the Country.

CHAPTER 3

The “Right to be forgotten”: a rightful challenge against the Internet.

Introduction:

In the era of small wavelengths and 5G internet, it can be said that 'What is uploaded on the internet, stays on the internet for eternity'. Cell phones or Mobile devices have become so accessible that any and all information about any person, object, or place is available with a single click on our devices, and we can access them from anywhere and at any time. The information provided by search engines and various social media platforms also acts as a provider of information that a person may want to keep private or may not want to reveal or share with the rest of the world, such as certain articles or news about crimes committed by that person in the past, or certain images or videos of incidents and times that the individual finds embarrassing, and so on. We all must have done, some kind of silly acts in our childhood or during any course of time, and as saying goes, our parents used to capture those moments in a form of photo or video. Now, imagine one of your friends got a hold of that photo or video and uploaded that on social media. It will be quite embarrassing right? These days, it's hard to avoid your past because personal data can spread swiftly or stay online forever, easily found through quick searches. The “Right to be forgotten” exists for those who wish to start afresh, and as our digital footprint gets bigger, this right is becoming more and more important. Would it be wise for us to reserve the “Right to be forgotten”? is the central query regarding the origins and nature of the “Right to be forgotten”. Various information about an individual that may be found on the internet, regardless of whether it is accurate, false, out of context, or factual at all, can be harmful to the person or act as a threat to their sense of autonomy or dignity. Protecting personal data that is available on the internet is a

complex issue that must be approached with caution owing to the fact that it is a sensitive but also highly significant component of a person's life and "Privacy".

As the internet becomes increasingly pervasive in modern life, questions concerning the "right to Privacy" in a digital world arise. The rights to free speech and public information are in conflict with the "Right to be forgotten", a new digital "Privacy" law designed to safeguard a person's ability to control how the internet defines her. The emergence of the "Right to be forgotten" reflects a fundamental paradigm shift in the human experience, from one in which forgetting was the default and the mind bore the sole burden of remembering and retaining, to one in which data in the digital world makes preservation the norm and forgetting a struggle.

We all realize that no matter wherever we are, our mind is in constant touch with digital world. Our longings find an easier path to connect through the realm of social media. So much so, that we do not realize when our personal data became more valuable than vast oil fields. The concept of 'right' has been acknowledged by many scholars as a cardinal requirement for the ultimate development of an individual and his intellectuality. Among such rights, "right to Privacy" is considered as one of the important rights necessary for the establishment of one's identity in a society. The Merriam- Webster dictionary defines the term '"Privacy"' as the quality or state of being apart from company or observation and the freedom from un-authorized intrusion.[78] As the definition suggests, "Privacy" is a right in rem which provides a person the authority to conceal any knowledge or data which he or she does not want to share with any other person. "Privacy", according to Judith Thomson,[79] is a collection of derivative rights, some of which are derived from the right to own or use one's

[78] Definition of '"Privacy"', Retrieved from www.merriam-webster.com/dictionary/"Privacy"

[79] Judith Jarvis Thomson,(1975) The Right to "Privacy", *Philosophy & Public Affairs* 295–314. Retrieved from www.jstor.org/stable/2265075

property, others from the “right to one's person” or the “freedom to decide what to do” with one's body, and so on. Thomson observed that “there is no such thing as violating a man’s right to “Privacy” by simply knowing something about him.” She justifies this with the argument that "None of us has a claim over any fact to the consequence that fact shall not be known by others." If knowing something about you violates your right to “Privacy”, it must be due to the method by which the truth was discovered; it is about the how, not the what, that is known about you. In the era of internet, where data is considered as the new liquid gold, it is very challenging to ensure proper security to one’s personal data. For instance, Cambridge Analytica “Data Breach”,[80] Yahoo “Data Breach” in 2013-14 impacted 3 Action users.[81] LinkedIn “Data Breach” in 2021 which saw a massive data loss of 700 million users[82] has drawn attention of global communities towards the need of a strong and robust sui-generis “Data Protection” laws for both domestic and international platforms.

What is “Right to be forgotten” and Why is it important?

The territoriality of law is challenged by the Internet. The global nature of the Internet poses a challenge to the right to erasure, or the “Right to be forgotten”, as defined by EU “Data Protection” law. Internet search engines and the fact that personal name searches expose more information covered by EU “Data Protection” law have contributed to the development of this right. The EU erasure right can require that search engines de-index protected personal information, but due to the accessibility of various search engine versions across legal boundaries, implementation could be seen as pitting the remedy's efficacy against

[80] Julia Carrie Wong (2019, March 18). The Cambridge Analytica scandal changed the world – but it didn’t change Facebook, *The Guardian.* Retrieved from www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook

[81] Edward J. (2018, May11) The Hacked & the Hacker-for-Hire: Lessons from the Yahoo “Data Breach”es (So Far).*The National Law Review*. Retrieved from www.natlawreview.com/article/hacked-hacker-hire-lessons-yahoo-data-breaches-so-far.

[82] Ode Holdings Inc. (2023, April 13), Top “Data Breach”es which effected millions of users. Retrieved from https://www.linkedin.com/pulse/top-data-breaches-which-effected-million-users-opendataeconomy

jurisdictional authority. Imagine a scenario where you may have committed a minor crime as a child and your name was listed as an accused in the local newspaper. But, the charges were shown to be false during your trial, and as a result, you were released from custody. Now, fifteen years later, as an adult, you discover all of your job applications are canceled due to that news article which is still available in the internet. Do you consider this to be just?

The desire to have personal information erased so that it can no longer be traced by outside parties is reflected in the "Right to be forgotten". It has been described as the freedom to remain silent about prior experiences that are no longer happening. The ability to have personal data, including images, videos, and photos, removed from some online records so that search engines cannot find them is known as the "Right to be forgotten"(Weber 2011).

How it can help:

Of course, the "Right to be forgotten" is fraught with difficulties. It might be tough to evaluate which material should be removed and which should be kept available. Furthermore, the "Right to be forgotten" may conflict with other vital rights, such as freedom of expression and the right of the public to know. Despite these obstacles, the "Right to be forgotten" is a crucial instrument in the digital age for protecting human "Privacy" and encouraging self-determination.

Not to be prejudiced: Employers, landlords, and other prospective decision-makers may utilize internet information to make decisions about someone, even if such information is outdated or incorrect. The "Right to be forgotten" can aid in preventing discrimination against individuals due to prior errors or offenses.

Protection against Harm of Character: It guards against reputational harm. Even if a person has done a mistake in the past, they should not be punished indefinitely for it. The

“Right to be forgotten” might assist individuals in moving on from their past and rebuilding their lives.

Encourages self-determination: Individuals should be able to control how their personal information is utilized. People have more control over their digital identities thanks to the “Right to be forgotten”, which allows individuals to choose what information about themselves is publicly visible.

The “Right to be forgotten” is not a perfect answer, but it is an important tool for those who want to protect their “Privacy”. Here are some particular examples of how individuals can be protected by the “Right to be forgotten”:

1. A person who was convicted of a crime many years ago and has now been rehabilitated may be eligible to ask search engines to delete links to news articles concerning their conviction.
2. A victim of revenge porn may be entitled to request that search engines remove links to the images.
3. A person who has been wrongfully accused of a crime may be entitled to ask search engines to remove links to websites that contain inaccurate material about them.

Discussion on the Historical Development of Right to be forgotten:

Development in Europe:

Europe, among its peers were the first to acknowledge the concept of “Right to be forgotten”, in the form of Right to erasure. To be more precise the European Union's “Data Protection Directive” (Directive 95/46/EC) in 1995 was the first legislation enacted by the EU. Individuals were granted the right to see their personal data, correct it if it was wrong, and

delete it if it was no longer required for the reason for which it was obtained. However, the need of a concrete jurisdiction in this field was felt during the year of 2014 when the European Court of Justice ruled in the case of Mario "Costeja González v Google Spain SL"(Floridi 2015)[83] Individuals have the right to approach data giants to make corrections in the relevant data related to them available in the data bank of data fiduciaries.

Facts of the Case: A Spanish man, Mario Costeja González, brought the test case "Privacy" ruling by the European Union's court of justice against Google Spain after he failed to secure the deletion of an auction notice of his repossessed home dating from 1998 on the website of a mass circulation newspaper in Catalonia. Costeja González contended that the case in which his house was auctioned off to recoup his social security arrears had been settled and that his name should no longer be associated with him whenever his name was searched on Google. The European Court determined that Google had to take down connections to two pages on La Vanguardia's website from Costeja González search engine results in accordance with current EU "Data Protection" laws. The Court stated unequivocally that the EU "Data Protection" legislation already established a ""Right to be forgotten"". This appears to foreshadow lengthy EU deliberations over a new data "Privacy" directive that might include a limited ""Right to be forgotten"." It was also determined that including links in Google results relating to an individual who requested that they be removed "on the grounds that he wishes the information appearing on those pages relating to him personally to be 'forgotten' after a certain time" was incompatible with existing "Data Protection" law. The Court held that- the data that had to be erased could "appear inadequate, irrelevant, no longer relevant, or excessive... in light of the time that had elapsed." They went on to say that even factual data that was initially legitimately disseminated could "over time become incompatible with the

[83] Floridi, Luciano. 2015. "'The "Right to be forgotten"': A Philosophical View." Jahrbuch Für Recht Und Ethik / Annual Review of Law and Ethics 23:163–79.

directive(Travis and Arthur 2014)[84]." In technical words, the verdict clarifies that a search engine like Google must be considered a "data controller" under “Data Protection” rules in EU nations when it establishes a branch to promote and sell advertising. They also stated that there is a balancing public interest defence against deletion, particularly if the individual is participating in public life. However, the judges argue that the role of a search engine in being able to build a "ubiquitous" list of results that can easily provide more or less thorough' profile of an individual's private life "heightens" the interference with “Privacy” rights. The verdict states unequivocally that a search engine, such as Google, must accept responsibility as a "data controller" for the content to which it links and may be obliged to remove its results, even if the material was previously published legally.

Role of GDPR:

The GDPR defines the specific circumstances in which the “Right to be forgotten” applies in “Article 17 of GDPR”[85]. An individual has the right to have their data removed if:

1. The personal data are no longer required for the original purpose for which it was acquired or processed by the organization.

2. An organization relies on an individual's consent as the legal basis for data processing, and that individual withdraws their consent.

[84] Travis, Alan, and Charles Arthur. 2014. “EU Court Backs ‘“Right to be forgotten”’: Google Must Amend Results on Request.” *The Guardian*, May 13.

[85] Anon. n.d. “Art. 17 GDPR – Right to Erasure (‘“Right to be forgotten”’).” *General “Data Protection” Regulation (GDPR)*. Retrieved November 1, 2023 (https://gdpr-info.eu/art-17-gdpr/).

3. An organization bases its processing of an individual's data on legitimate interests, the individual objects to the processing, and there is no overwhelming legitimate interest for the organization to continue the processing.

4. A business handles individual objects and “personal data” for direct marketing reasons.

5. An organization unlawfully processed an individual's personal data. to comply with a legal rule or requirement, an organization must remove personal data.

6. An organization has processed a child’s personal data to offer their information society services.

The GDPR cites the following grounds that outweigh the “Right to be forgotten”:

1. The data is being used to exercise the right of “freedom of expression and information”.

2. The data is being used to comply with a legal ruling or obligation.

The data is being used to perform a task that is being carried out in the public interest or when exercising an organization’s official authority.

3. The data being processed is necessary for public health purposes and serves in the public interest.

4. The data being processed is necessary to perform preventative or occupational medicine. This only applies when the data is being processed by a health professional who is subject to a legal obligation of professional secrecy.

5. The data provides critical information that serves the public interest, scientific research, historical research, or statistical purposes, and deletion of the data is likely to impede or prevent progress towards the achievement that was the processing's goal.

6. The data is being utilized to develop a legal defense or to pursue other legal claims. Furthermore, GDPR standards allow an organisation to request a "reasonable fee" or deny a request to delete personal data if the organisation can demonstrate that the request was baseless or disproportionate.

In "*Google LLC v Commission Nationale de l'Information et des Liberties (CNIL")*[86] the European Court held that right to erasure is limited by a certain territorial jurisdiction and the data fiduciary is not liable to acknowledge this right through out the globe. Google received official notice on May 21, 2015, from the President of the Commission nationale de l'informatique et des libertés ("CNIL"), the French "Data Protection" authority, stating that the company must honour requests to remove search results from the global search results rather than just the domain of the requester's residence. Google declined and restricted the removal to EU members only. The business claimed that authoritarian governments might take advantage of global removal. A *"geo-blocking technique"* was suggested by Google to stop users in EU Member States from visiting links that have been delisted within the EU. CNIL fined €100,000 for finding these actions to be insufficient. Google filed an appeal with the Conseil to have the CNIL's decision overturned.

The EU General "Data Protection" Regulation of 2016 ("GDPR") and the EU "Data Protection" Directive of 1995 ("DPD") were taken into consideration by the Court in making its decision. Due to its operations in French territory, the Court first determined that Google was subject to the DPD and GDPR. The objective of the applicable EU law was then taken into consideration, which was to ensure a "high level of protection of personal data throughout the European Union." However, the public interest in information access and other "fundamental right" must be taken into consideration when weighing the right to

[86] "CURIA - Documents." Retrieved November 1, 2023 (https://curia.europa.eu/juris/document/document.jsf?text=&docid=218105&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=2884415).

personal “Data Protection”. The Court concluded that it could not enforce EU legislation outside of Member States due to the international nature of the internet and nations' varying perspectives on striking a balance between the right to information and the “Right to be forgotten”. Search engines must, however, "effectively prevent" or "seriously discourage" all users in the Member States from accessing the de-listed links through non-Member-State domains if they accept a request to be removed from the list[87].

USA and Its Journey towards “Right to be forgotten”:

“Griswold v. Connecticut”[88] is a significant case that helped establish the right to “Privacy” in US history. The right to “Privacy” in marriage was declared to be breached by a Connecticut legislation that forbade the use of contraceptives, according to a ruling by the US Supreme Court. This 1965 decision established the rights of private individuals in the United States to “Privacy”, especially the rights of a married couple in their own private relationship. Fourth Amendment rights are "creating a right to “Privacy”, no less important than any other right carefully and particularly reserved to the people," the Court held in the Griswold case.[89].

The US Apex Court interpreted the Fourth Amendment in “**Katz v. United States”**[90], two years after Griswold, to confirm that people are protected from arbitrary searches and seizures by the amendment. In this instant case the government installed a listening device on the phone booth to record Mr. Katz's conversations and his statements to the parties he was speaking to while he was making calls in a public phone booth because they believed he was engaged in some illegal activity. The Court ruled that because Katz was protected from arbitrary searches and seizures by the Fourth Amendment, the government could not listen in

[87] 6 Case C-507/17, Google LLC v. Commission nationale de l’informatique et des libertés (CNIL), ECLI:EU:C:2019:772, ¶ 39 (October. 21, 2023) (judgment).

[88] Griswold v. Connecticut, 381 U.S. 479, 484–86 (1965).

[89] William M. Beaney, The Constitutional Right to “Privacy”, 1962 SUP.CT. REV. 212 (1962). See also Erwin Griswold, The Right to Be Let Alone, 55 NW. U. L. REV. 216 (1960)

[90] Katz v. United States, 389 U.S. 347, 359 (1967).

on his private conversations even though he was using a phone booth. For the government to install a listening device in the phone booth, they had to show reasonable suspicion. The Court ruled that the listening device constituted an unreasonable search because it violated the government's Fourth Amendment prohibition on unreasonable searches and seizures. Because he was confined to a room and could reasonably expect his calls to remain private, Katz depended on the idea that they were private. Katz was right when the court determined that the government was infringing on his right to “Privacy”.

The Supreme Court addressed the prohibition imposed by the Fourth Amendment on using technology for public surveillance in **Kyllo v. United States**[91]. According to the Court, if "(1) the information would not have been collected from a legal vantage point and (2) the technology is not generally available to the public," then the government could not use technology to invade someone's “Privacy”. The government thought Kyllo was cultivating marijuana plants in his house, so they used a gadget to find heat lamps in his house. The device used to detect the lamps was not in "general public use," and that device revealed details of the home that would otherwise be "unknowable" without physically entering the house, according to the Court, which held that the thermal technology used to gather information from the interior of the home constituted an unreasonable search. Therefore, this type of search was forbidden by the Fourth Amendment.

The introduction of Google Street View in 2007 has created yet another avenue for “Privacy” violations in the Internet age. Funny pictures and videos taken by Google's own mobile phone while it was participating in the Street View program can be found all over YouTube. Given that the “United States of America” is a very "legally sound Country," a couple decided to sue Google for its Street View program. All classes of citizens are quite concerned about this

[91] 7 Kyllo v. United States, 533 U.S. 27 (2001)

case, despite its humor. The Boring v. Google[92] case raised new issues for the court to consider in this new technological era following the release of Google Street View. A husband-and-wife team named The Borings sued Google over the company's Street View initiative. Google drove around cities with cars equipped with cameras to capture images of the surrounding area. Google had captured "colored imagery of their residence, including the swimming pool from a vehicle in their residence driveway months earlier without obtaining any “Privacy” waiver or authorization, from the Boring family, who lived on that private road. The Borings said that Google had violated their right to “Privacy” by making the Street View camera's images publicly accessible online and by posting "No Trespassing" signs on their street. The Borings' right to “Privacy” was not violated, the court ruled, by Google. Street View was not likely to qualify as a search under the terms of the Fourth Amendment for two reasons: "First, photos such as those taken by Google and posted on Street View are not more detailed than what the human eye could see while strolling down the same street. Second, millions of people can now access the 360-degree car camera technology that Google uses online. Nowadays, it is reasonable to assume that surveillance cameras or apps like Street View will be watching people in public areas. Because of Griswold and Katz, courts are quick to defend people's “Privacy” when they are in private settings. However, when they are not, the courts are more likely to decide that public information does not violate someone's right to “Privacy” or the Fourth Amendment, as was the case in the Boring case mentioned above.

[92] Boring v. Google Inc., 362 F. Appx. 273, 276 (3d Cir. 2010).

Challenges Before 'Right to be Forgotten' to be acknowledged as a Right under Right to "Privacy":

The First Amendment is another obstacle that the "Right to be forgotten" movement in the US faces. The US courts have steadfastly maintained the right to free speech as a core constitutional right. In 1953, a Californian court considered an infringement of "Privacy" in a public setting. Gill v. Hearst Publishing Company concerns a Harper's Bazaar reporter who took a photo of a couple at a farmer's market. In an article about love, the magazine included a picture of the couple that showed them cuddling. The couple, who were embracing, had no idea that the magazine was taking their picture, much less given their permission. After learning, the couple asserted their right to "Privacy" and their right to prevent the photo from being released. The couple's "right to be left alone," "public interest in the dissemination of news," and ""The "Freedom of Speech"" and the press" were all taken into consideration by the court in a balancing test. The couple decided to be in public and show their love, so the court ruled that the photo did not violate the plaintiff's right to "Privacy". The court placed greater weight on the right to free speech in this case than the couple's right to "Privacy" in a public setting. This case supports the preceding discussion regarding the Fourteenth Amendment. The court was more willing to defend the magazine company's "free speech" because the couple was displaying their "affection for one another" in public rather than in the "Privacy" of their own home, which meant they did not have the right to "Privacy" in a public place[93].

The U.S. Court of Appeals for the Second Circuit rendered a decision in 2015 regarding internet "Privacy" and information. Lorraine Martin was detained on suspicion of drug

[93] Leticia Bode & Meg Leta Jones, *Ready to Forget: American Attitudes toward the "Right to be forgotten"*, 33 THE INFORMATION SOCIETY 76 (2017).

offences in **Martin v. Hearst Corporation**[94]. Although Martin was not charged by the state, her arrest was covered in an online news article because she was there with her two kids. Martin asked that the news media remove the articles about her because she believed them to be untrue because she was not ultimately charged with the crime, effectively erasing and expunging her charges from her record. Martin filed a lawsuit after the media declined to take down the articles. The Court of Appeals ruled that just because the defendant is later found to have never been arrested as a matter of legal fiction, the law of erasure does not make historically accurate news accounts of an arrest tortious. The court went on to say that since the articles did not present false information, it would be unlawful to order the media to take the content down from the internet in violation of the First Amendment.

Martin emphasized that the courts are much more likely to uphold the publication of saleable news under the US First Amendment, even when that information may have a detrimental impact on an individual's life. This case provides a glimpse into why American law does not systemically incorporate the "Right to be forgotten".

On the Path of Change:

1978 saw the adoption of the Act on Information Technology, Data Files, and Civil Liberties by the National Assembly. The legislation protected a person's right to object to the publication of their personal information online. This law allowed people to request that the data controller update, correct, block, or remove any inaccurate or out-of-date personal information by presenting proof of identity[95].

The ECJ rendered a decision in 2019 regarding a novel facet of the "Right to be forgotten". The EU's "Right to be forgotten" regulations were expanded by the Google LLC, Successor

[94] Martin v. Hearst Corp., 777 F.3d 546, (2d Cir. 2015)

[95] Shaniqua Singleton, Balancing A "Right to be forgotten" with A Right to Freedom of Expression in the Wake of Google Spain v. Aepd, 44 Ga. J. INT'L & COMP. L. 165, 176 (2015).

in Law to “Google Inc. v. Commission Nationale de L'informatique et des Libertés” (CNIL) case. Google was fined 100,000 euros by the French “Data Protection” authority CNIL in 2016. This was due to Google's denial of a request to apply to all of its search engines worldwide, which would have removed results associated with an individual's name from search results. When Google rejected a request in 2016, the erasure was only taken down from the search engines in the member states. The court later on reiterated that the right to personal “Data Protection” is not an absolute right but rather needs to be weighed against other “fundamental right”in accordance with the proportionality principle and in relation to its role in society. Furthermore, "the balance between the freedom of information of internet users and the protection of personal data and the right to “Privacy”, on the one hand, is likely to vary significantly around the world." As of right now, a search engine like Google that accepts a request for de-referencing from an individual is not required by EU law to perform that dereferencing across all of its search engine versions.[96]

To protect its inhabitants, the USA has constructed a complicated set of rules. “*Act A05323”* was swiftly introduced in New York. Furthermore, in March 2017, New York State representatives Tony Avella and David Weprin proposed legislation that would allow people to request that web search engines and online speakers remove information that is 'off base,' 'insignificant,' 'deficient,' or 'excessive,' that is "as of now not material to energize public discussion or talk," and that is harming the subject.

However, search engine operators are required by EU law to implement de-referencing on the versions of their search engine that are utilized in each of the member states and to take "sufficiently effective measures" to guarantee that the “fundamental right”of individuals are protected. Google won this case because, at least for the time being, it is not required to

[96] Court of the European Union, Press Release No. 112/19: Judgment on Case C507/17, The Operator of a Search Engine is Not Required to Carry out a Dereferencing on All Versions of its Search Engine, Sept. 24, 2010, https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-

implement the “Right to be forgotten” in the United States. It is not necessary for Google to take down search results that a member state has devalued and then apply that modification to the search results in the US.

As the saying goes, ‘Change is inevitable’. Now google has decided to change it’s policies regarding erasure of data and become more user friendly. The “Right to be forgotten” is not formally recognized by legislation in the United States. However, there are a variety of statutes and case law that protect individuals' online “Privacy” rights. The California Consumer “Privacy” Act (CCPA), for example, allows customers the right to have corporations that gather their personal information remove it. Furthermore, several states have laws that expressly restrict the internet publication of certain sorts of personal information, such as revenge porn. In addition to statutory safeguards, a growing body of case law recognizes individuals' right to “Privacy” online. Consider the 2018 case of Doe v. Google. The California Supreme Court ruled that people can sue search engines for defamation if they post links to erroneous or outdated material about them.

“Right to be forgotten” as a Part of Right to Life “U/A 21 of the Indian Constitution”:

The largest obstacle to the "“Right to be forgotten”" in India at the moment is the right to information. The rights to “Privacy” and knowledge are the two most important rights in India to guarantee that people can live their life with honor and honesty. These two rights are essential to guaranteeing a person's standard of living. The right to hold government agencies responsible for major public concerns differs with the right to “Privacy”, which allows people to keep their personal problems and situations secret. These two rights typically operate in concert to keep the government answerable to the people. These rights, however, collide when someone requests access to private data held by government agencies.

A collection of procedures and guidelines that can be applied to safeguard the confidentiality, accessibility, and integrity of data is known as “Data Protection”, sometimes referred to as data security or information “Privacy”. In the digital age, data is present everywhere and may be seen in many different ways. For example, we have to enter our name and address when we shop online. Sometimes gathering data is less obvious. Consider data brokers, for instance. Most of us have never heard of them, but these businesses are experts at creating comprehensive profiles of people for marketing purposes. Up to 1,500 data points, including a person's sexual orientation, browsing history, political affiliation, and even medical information, can be found in a single profile. The handling of public data by third parties, including its collection, processing, sharing, archiving, and usage, is the subject of “Data Protection”. We could argue that “Data Protection” is a subset of “Privacy” and has a greater impact on an individual's life, and that “Privacy” and “Data Protection” are interwoven. Although “Data Protection” is more precisely defined than “Privacy”, its use in compliance with national “Privacy” laws varies depending on the legal frameworks of the various countries. Following the Aadhar judgement, which also introduced the concept of “Data Protection”, India recognized the right to “Privacy”. India does not have a formal “Data Protection” law, therefore any data and information provided or received must be interpreted in accordance with a patchwork of rules, regulations, and guidelines. “The Information Technology Act of 2000”, widely recognized as the foundational legislation addressing cybercrime and electronic commerce, is the most significant and well-known. Information exchanged in non-electronic form is not covered by these laws and guidelines; only information shared electronically is. This rule's scope is constrained, nevertheless, and it mainly applies to private information that is collected through sensitive corporate computer systems “The “DPDP Act”'s” implementation seems to have altered the circumstances. By forcing data fiduciaries to store their data locally and requiring them to get consent from

ground level stakeholders, or data customers, before storing their data, the Act seeks to put more of an emphasis on “Data Protection”.

In India, Article 19's “fundamental right” to “Freedom of Speech” and expression serves as the basis for the right to knowledge. Numerous incidents have shown that everyone's right to the freedom of knowledge is guaranteed by the “Indian Constitution” and is a basic component of that document. As a result of RTI's constitutional status, it has been enshrined in law as the “Right to Information Act, 2005”, which focuses on government agencies' disclosure of information to the public interest or in response to community needs. This act protected the “Privacy” of citizens and well-known individuals while simultaneously establishing designated officers to answer public inquiries, a complaint procedure, and proactive government publication of certain kinds of information. The Supreme Court's rulings in cases like “Bennett Coleman and Co. v. Union of India”, where it was decided that the right to information was part of “The “Freedom of Speech” and expression protected by “Article 19(1)(a)”, demonstrate the evolution of the right to information. The case of “SP Gupta vs. Union of India” then explained the people's right to know about every public act and the specifics of every public transaction carried out by public personnel. Thus, the public's ability to obtain information from the government or other public body that serves the public interest is seen as a “fundamental right” that has been acknowledged and accepted as a legal right in India.

It is well known that the government holds many private documents belonging to a variety of people. Authorities may have access to a person's income tax returns, clinical records, biometric data, and other personal possessions. An individual's “Privacy” will be gravely breached if such records are made available through the RTI process. However, it also makes an effort to make sure that no one pretends to be private or safe to shield themselves from having their data disclosed, which may be required by RTI. The applicant must prove to the

public information officer that the data is of public interest and that disclosing it will benefit the public at large in situations where there is debate about whether the data should be safeguarded under “Section 8(1)(j)”. If the officer is happy, the data can be disseminated. In this instance, an individual's right to “Privacy” is superseded by the interests of the wider public. This could lead to a contradiction between these rights. The question is whether these rights are incompatible with quantity to the point where they cannot be reconciled. There have been numerous attempts, with differing degrees of success, to unify these provisions. These rights could be complimentary to one another, pushing government officials to be more accountable and transparent.

We've all had humiliating times in our lives and made mistakes we're not proud of. Many of us grow and change. But what if the rest of the world ignores our progress? This is the essence of the concept of the “Right to be forgotten”. People believe that humans are autonomous beings with a natural need for “Privacy” and control over certain areas of their lives. Since we live in this day and age, our data is easily accessible via the internet or public forums. As a result, everyone must work together to secure it. The issue over “Data Protection” and “Privacy” in India was established by the decision of Justice “K.S. Puttaswamy v. Union of India”[97], in which the Supreme Court recognised the right to “Privacy” to be a “fundamental right”. Standing and Parliamentary Committees have also underlined the necessity for particular “Data Protection” and “Privacy” rules in their recommendations. The “Justice B.N. Srikrishna Committee” proposed a new “Data Protection” Act in May 2018. The proposed legislation delves into the concept of a relatively new right, the '“Right to be forgotten”,' which seeks to protect personal data. The “Right to be forgotten” Personal information such as photographs, videos, and other personally identifiable data can be removed from publicly available sources such as internet searches

[97] MANU/SC/0911/2017

and other web-based directories under specific situations. Businesses that have sensitive personal data but fail to keep it secure, resulting in anyone's unlawful loss or unjust gain, may be forced to compensate the individual who was affected, according to "Section 43A of the Information Technology Act of 2000". The "Right to be forgotten" is not explicitly included in the Government of India's notification of the "Information Technology Intermediary Guidelines and Digital Media Ethics Code Rules 2021". It does, however, offer procedures for filing complaints with the designated Grievance Officer to have content revealing personal information about the complainant deleted from the internet without the complainant's agreement[98].

In the case of "**Dharamraj Bhanushankar Dave v. State of Gujarat & Ors" (2015)** before the Gujarat High Court, the "Right to be forgotten" was first raised. In this case, the petitioner was accused of criminal conspiracy, murder, and kidnapping and was acquitted by the Court; thus, he requested that the respondent be prohibited from publishing the non-reportable judgement on the internet, as it could harm the petitioner's personal and professional life. as it was causing defamation However, the court refused to accept the '"Right to be forgotten"' in India.

The '"Right to be forgotten"' was asserted once, in the case **of "Jorawar Singh Mundy vs. Union of India" (W.P. (C) 3918/ 2020)**, in which the Single Judge bench comprised of Justice Pratibha M. Singh held that, on the one hand, there is the petitioners' right to "Privacy" and, on the other hand, the public's right to information and the preservation of transparency in judicial records. However, the court prioritized the petitioners' rights.

On October 9, 2023, India lost nearly 81 million of its citizens' data to the darkweb. It has been revealed that the data of patients collected by the ICMR (Indian Council for Medical

[98] Is The '"Right to be forgotten"' a "fundamental right"?, THE TIMES OF INDIA, https://timesofindia.indiatimes.com/readersblog/myblogpost/is-the-right-to-be-forgotten-a-fundamental-right-52529/ (last visited Nov 2, 2023).

Research) was taken by a hacker known as PWN0001. Name, Father's name, Phone number, Other number, Passport number, Aadhaar number, Age" are among the disclosed details. This data is expected to cost about $80,000 in total. If this was enforced before, people may have had the option to erase their data after the covid period was over. It will not be wrong to say that government bears the responsibility to protect its citizens from every kind of threat. This right here is a digital threat, and the Government is duty bound to protect it's citizens from such threats. We know that the new "DPDP Act" 2023 has been adopted by the Indian Government, however it will take few more years to properly implement them. Under the new act a customer can formally request the data fiduciary to erase his/her data from their online platforms, provided the following requirements are matched:

1. The subject has withdrawn their permission to the processing of their personal data.
2. The personal data is no longer required for the purpose for which it was acquired or processed.
3. The personal data has been processed unlawfully.
4. On valid grounds, the subject objects to the processing of their personal data.

Personal data fiduciaries are required to destroy personal data within a reasonable time after receiving a legitimate request from an individual. However, there are some exceptions to the "Right to be forgotten", such as when the personal data is required for the performance of a legal duty or the establishment, exercise, or defense of legal claims. Individuals can exercise their right to erasure by submitting a written request to the data fiduciary. The request should describe the personal data to be erased as well as the rationale for the request. The data fiduciary must respond to the request within a reasonable timeframe. If the data fiduciary refuses to destroy the individual's personal data, the individual may submit a complaint with

the “Data Protection” Board of India, the regulating agency established by the “DPDP Act”. The “Data Protection” Board has the authority to investigate a complaint and issue orders requiring the data fiduciary to comply with the law. The “Right to be forgotten” is a crucial right that grants individuals control over their personal data. It contributes to ensuring that individuals are not obliged to keep their personal data with data fiduciaries who are untrustworthy or who are not using the data lawfully.

Conclusion:

“Privacy” is a fundamental human right, yet computer systems hold huge volumes of potentially sensitive data. The Information Technology Act's Chapters IX and XI define liabilities for data confidentiality and “Privacy” violations involving unauthorized access to a computer, computer system, computer network, or resources, unauthorized alteration, deletion, addition, modification, destruction, duplication, or transmission of data, computer databases, and so on. Financial information, health information, business plans, intellectual property, and sensitive data may all be protected. Today, however, anyone can access any information on anyone from anywhere at any time, posing a new threat to private and protected information. Globalisation has given technology worldwide acceptance. distinct countries have adopted distinct legal frameworks like “DPA” (“Data Protection Act”) 1998 UK, ECPA (Electronic Communications “Privacy” Act of 1986) USA, etc. as per expanding requirements. Special “Privacy” laws exist in the United States to safeguard student education records, children's online “Privacy”, individuals' medical records, and private financial information. Self-regulation activities in both countries are assisting in defining improved “Privacy” environments. The right to “Privacy” is recognized in the Constitution, but its expansion and development are entirely at the discretion of the judiciary. In today's

interconnected society, it is incredibly impossible to keep information from leaking into the public realm if someone is motivated to do so without resorting to extremely harsh measures. The Information Technology (Amendment) Act of 2008 addressed “Data Protection” and “Privacy”, although not exhaustively. The “IT act”must specify clear requirements for the means and purposes of assimilation of the right to “Privacy” and personal data. To summarize, the “IT act”faces the problem of “Data Protection”; however, the “DPDP Act” can protect Indian consumer data within its territorial jurisdiction, and a separate sui generis global legislation striking an effective balance between personal liberties and “Privacy” is much needed.

CHAPTER 4

Data “Privacy” and Protection of Personal Data in India.

Introduction:

The concept "“Privacy”" is difficult to grasp while considering its definition. It has been interpreted in a variety of ways. "Right to “Privacy”," according to Black's Law Dictionary, covers "various Rights recognized as inherent in the concept of ordered liberty." These liberties safeguard people's “fundamental right” to choose how they wish to spend their lives and engage with their families, other people, and interpersonal connections and activities. Additionally, it has been said that “Privacy” is the legal right of an individual to decide how much of themselves they wish to disclose to third parties and to decide when, where, and under what conditions they choose to do so. It refers to his unlimited ability to participate or not participate in whatever way he sees fit. It also refers to the individual's right to choose what information about him or her is made public; he or she is the exclusive proprietor of that information. A person's "Right to be Left Alone," on the other hand, denotes the right to “Privacy”.

The Concept of “Privacy”: The concept of “Privacy” extends back to the origin of human civilization. However, the concept of “Privacy” is difficult to grasp. For different scholars, the term "“Privacy”" has taken on a number of meanings, and those definitions evolve as society itself does. Its origins can be traced back to debates in the “Constituent Assembly” on ‘*“Privacy and secrec”*. The deliberations in the “Constituent Assembly” make it evident that the Right to “Privacy” was purposely removed from the Constitution. The reasons of legislators are unknown. The Right to “Privacy” is not specifically recognized in India's post-independence Constitution, but precedents in the courts have allowed it to develop. It was

acknowledged for the first time in "the case of **Kharak Singh"**[99]. It is a well-known fact that Indian laws draws their enforceability from the Indian constitution, therefore before we start discussing about them, it is very important to understand about the constitutional essence of Right to "Privacy" first. "The Right to Privacy" has evolved under the umbrella of Indian Constitution under the heading of "affirmative action", and the Indian Judiciary had also played a crucial rule in the process. For instance, "**In R. Rajgopal v State of Tamil Nadu"**[100], The Indian Supreme Court ruled that the right to "Privacy" is a "fundamental right" guaranteed by "Article 21 of the Indian Constitution", acknowledging the right to "Privacy" in a range of circumstances. Consequently, each person has the right to private protection and the freedom to be by themselves or with their family. The Right to "Privacy" was recognized in "**People's Union for Civil Liberties (PUCL) v Union of India"**[101] under "Article 17 of the ICCPR" and "Article 12 of the UDHR". The Supreme Court further highlighted that, while the "Indian Constitution" did not directly provide for a right to "Privacy", it was a component of the right to "life" and "personal liberty" under Article 21, which could not be restricted "except in accordance with the procedure established by law." The Court stated that the right to hold a telephone conversation in the "Privacy" of one's home or office without interference can certainly be claimed as a right to "Privacy" and concluded that telephone tapping would violate "Article 21" unless approved by a "procedure established by law." The Court also said that telephonic conversations were an exercise of a citizen's right to free speech and expression under "Article 19(1)(a)", and hence interception of these conversations had to be a justifiable restriction under Article 19(2) of the Constitution. The Supreme Court once again recognized the Right to "Privacy" as an inherent

[99] Kharak Singh vs The State of U. P. & Others on 18 December, 1962, https://indiankanoon.org/doc/619152/ (last visited Jun 9, 2023).
[100] Rachit Garg, *R. Rajagopal and Ors. v. State of Tamil Nadu, 1994 SCC (6) 632 : Case Study*, IPLEADERS (Jan. 28, 2022), https://blog.ipleaders.in/r-rajagopal-and-ors-v-state-of-tamil-nadu-1994-scc-6-632-case-study/ (last visited Jun 9, 2023).
[101] People's Union for Civil Liberties vs. Union of India & Ors., https://"Privacy"library.ccgnlud.org/case/pucl-vs-union-of-india (last visited Jun 9, 2023).

aspect of Article 21 in "**Ram Jeth Malani v Union of India"**[102]. As pointed forth in "**Maneka Gandhi v Union of India"**[103], the right to "Privacy" is a basic right that falls under the purview of the right to life and personal liberty under Article 21 and can be curtailed by a mechanism established by law that is just, fair, and reasonable. It was established in "**Govind v State of MP"**[104] that the "fundamental right" explicitly given to a person has a multitude of zones and that the right to "Privacy" is itself a "fundamental right" that must be susceptible to restriction on the basis of compelling public interests. It is obvious from all of the case Laws reviewed that the Indian judiciary has developed the concept of "Privacy" as a broad phrase. The "Privacy" should be interpreted broadly; it should encompass bodily autonomy, making choices in topics deemed personal, and, of course, one's personal information. Within the confines of Article 21, the right to "Privacy" can be reduced only in extreme situations, in the absence of compelling state interest, and if it meets the **proportionality** test laid out in the "**Justice Puttaswamy** judgment". This one particular case was like a cherry on the icing of a cake, The Supreme Court affirmed that "the Right to "Privacy"" is a cornerstone of our Constitution in this case as well as others. In 2017, a five-judge panel of the Supreme Court while hearing the case involving the Aadhaar card and the "Right to "Privacy"" announced that they wanted a nine-judge panel to first determine whether "the Right to "Privacy"" is a basic right, before deciding on the main issue of Aadhaar. The Attorney General in the Aadhaar case noted that while previous judgments recognized the "Right to "Privacy"," they did not clearly recognize it, as in the Kharak Singh and M P Sharma rulings. As a result, a 9-judge bench must be formed to determine whether "the Right to "Privacy"" qualifies as a

[102] Ram Jethmalani and ors. vs. Union of India, https://"Privacy"library.ccgnlud.org/case/ram-jethmalani-and-ors-vs-union-of-india (last visited Jun 9, 2023).
[103] Mariya Paliwala, *Maneka Gandhi v. Union of India, 1978 AIR 597 1978 SCR (2) 621 197*, IPLEADERS (Dec. 23, 2019), https://blog.ipleaders.in/maneka-gandhi-v-union-of-india/ (last visited Jun 9, 2023).
[104] Govind vs. State of Madhya Pradesh & Ors., https://"Privacy"library.ccgnlud.org/case/g (last visited Jun 9, 2023).

fundamental freedom. It was the moment when the observation of the Apex Court started a rush of legislative proposals aimed at enacting Personal "Data Protection" Laws.

Recently, in the aftermath of Puttaswamy, other High Courts across the nation have grappled with the exercise of different aspects of "Privacy" rights. Recent High Court decisions on the contours of the right to erasure and the "Right to be forgotten" through remarkable judgments like **Subhranshu Rout @ Gugul v. State of Odisha** [BLAPL No. 4592 of 2020], **Sri Vasunathan v. the Registrar General, High Court of Karnataka and Ors** [General Writ Petition No. 62038 of 2016], and **Dharamraj Bhanushankar Dave v. State of Gujarat and Ors** [SCA No. Each of these courts took a different opinion, and it is safe to speculate that the scope and effects of these rights will continue to be disputed in court until new legislation is passed.

Protecting data of individual citizen is important for the state, but it is also important that, the Government must protect the State from any internal as well as external threats of any kind. This threat may include physical threat or economical threat. Physical threat includes threat of any kind of actions which can result into loss of life and Economical threat may include Loss of Intellectual Property or Technological Know hows. One must ask whether dwelling with personal data of citizens can be a method of ensuring security of the nation. Concerns about who is allowed to review our information, where it is stored, and purpose of usage of that data have grown among governments, businesses, and consumers with the introduction of the internet and other technologies. National security, business expansion, geopolitical ties, and civil society can all be significantly impacted by the manner in which data is gathered, maintained, utilized, and transmitted. Stakeholders argue that customer protection and comfort should be given during data processing and storage procedures, and that data should be secure. The need to guarantee secure and safe data storage is driving nations to enact "Data Protection" laws that strike a balance between national security and sovereignty and

economic innovation and globalization. Policies or laws requiring specific data connected to people or residents of a country whether personal, health, business, or financial—to be physically stored on infrastructure within that country's boundaries are the most widely recognized definition of "data localization." Mandates for data localization differ significantly between nations, contingent upon the goals of the governmental bodies that implement them. With the rise of technology and digitization, more countries are adopting data localization laws due to concerns that their sovereignty may be jeopardized if they cannot fully control the data that is held outside of their borders. These laws aim to restrict foreign governments' access rights to data stored outside of their jurisdiction, and they are motivated by worries about meddling from foreign governments. Attempting to reconcile the interests of stakeholder communities on data “Privacy”, human rights, and trade, democratic governments have supported and opposed similar laws. Increased surveillance and censorship of their citizens is made possible by the ostensible justifications provided by more authoritarian governments (and some democracies) for tightening control over their national digital infrastructure, including counterterrorism and limiting foreign influence. There are arguments for and against localizing data in terms of national security. The fundamental argument in favor of data localization is that the national security of its geopolitical rivals may be threatened by the unrestricted flow of data to autocratic or hostile governments. This might be illustrated by the fact that, because to their tense political ties with China, the US and India have justifiable worries about Chinese-owned businesses accessing the personal information of their residents. For example, India had banned a considerable amount Chinese owner apps like tiktok, Vigo etc to protect her **data sovereignty**. Second, since there isn't agreement on what national security concerns related to data localization actually are, some countries could be able to argue for stronger regulations.

Existing Laws in the Field of "Data Protection":

European Laws: General "Data Protection" Regulation is governing the "Data Protection" system in Europe. The 1950 European Convention on "Human Rights", which declares that "Everyone has the right to respect for his private and family life, his home, and his correspondence," includes the right to "Privacy". Based on this idea, the European Union has worked to enact laws that guarantee the "protection of this right". With the development of technology and the invention of the Internet, the EU realized that new protections were required. Thus, it passed the European "Data Protection" Directive in 1995, which set minimum standards for data security and "Privacy". Each member state then based its own implementing legislation on this directive. But the Internet was already changing, becoming the data-hungry place it is today. Facebook first opened to users in 2006. A Google user filed a lawsuit against the company in 2011 for email scanning. The EU required "a comprehensive approach on personal "Data Protection"," according to Europe's "Data Protection" authority, and work on updating the 1995 directive started two months later[105].

Principles of "Data Protection" in EU: EU as a union and members of EU on their individual capacity provides a strong system of "Data Protection" for their citizens. This system is based on principles like transparency maintained by the law makers as well as data fiduciaries, maintaining lawfulness and fairness in data processing, limitation of collecting personal data to a certain extent, prior informed collection of consent and providing proper information to individuals regarding storage of their data and being accountable regarding handling of data.

[105] What is GDPR, the EU's new "Data Protection" law?, GDPR.EU (2018), https://gdpr.eu/what-is-gdpr/ (last visited Oct 27, 2023).

Application: "Article 3 of GDPR" states that, the act is applicable to all and sundry if they have some kind of connection with the data of EU citizens. Let us discuss it further. "**Article 3"**[106] states that:

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

According to "Article 3.1", even if data is being used or stored outside of the EU, organisations with EU headquarters are still subject to the GDPR. "Article 3.2" goes a step further and applies the law to non-EU organisations as long as two requirements are satisfied: either the organisation provides goods or services to individuals within the EU, or it keeps an eye on their online activity. "Article 3.3" discusses fewer common situations, like those in EU embassies. Products and services located in remote locations are now available to everyone worldwide thanks to the Internet. For example, If I as an Indian order any food for

[106] Art. 3 GDPR – Territorial scope, GENERAL "DATA PROTECTION" REGULATION (GDPR), https://gdpr-info.eu/art-3-gdpr/ (last visited Oct 27, 2023).

one of my friend staying at Germany from a German food outlet, than “GDPR laws” will be applicable on me. But in isolated cases, the GDPR does not apply. Instead, regulators seek out additional hints to ascertain whether the company intended to provide goods and services to consumers in the EU. To accomplish this, they will check for things like whether a Indian business, for instance, made advertisements in German or put prices in euros on its website. To put it another way, you should work towards “GDPR compliance” if our business serves clients from the EU but is not located in the EU. Your organisation is subject to the GDPR if it makes use of online tools that let it track cookies or the IP addresses of visitors from EU nations. It's unclear how strictly this clause will be interpreted in practise or how blatantly it will be enforced. Let's say I own a online computer assembly line-up in Kolkata that caters only to India, but occasionally visitors from France find your website. Would I find myself targeted by regulators in Europe? It is unlikely. However, tracking these data could theoretically result in us being held responsible. Irrespective of these restriction, GDPR allows personal businesses and businesses having less than 250 employees to function without following the prescribed guidelines.

Sanctions:

The GDPR assigns administrative penalties to each EU member state's “Data Protection” regulator. That authority will decide the severity of the penalty and whether an infringement has occurred. The following criteria will be applied to decide whether and how much of a fine will be imposed:

1. The full picture of the breach, including its nature and effects. What happened, how it happened, why it happened, how many individuals were affected, what kind of harm they suffered, and how long did it take to resolve?

2. Reformative Action: Whether the company made any efforts to lessen the harm that the infringement caused to those who were impacted.
3. Preventive measures: How far the company had gone in terms of organisational and technical readiness to comply with the GDPR.
4. Co-operation: Whether or not the company complied with prior administrative corrective actions under the GDPR and collaborated with the supervisory authority to identify and address the infringement, as well as supplied the required information regarding any pertinent prior infringements, including violations under the "Data Protection" Directive (rather than just the GDPR).
5. Data category: What type of personal data the infringement affects.
6. Notification: Whether the company alerted the supervisory authority to the infringement on its own initiative or through a designated third party.
7. Certification: Whether the company had a prior certification or adhered to established codes of conduct.
8. Aggravating/mitigating factors: Any other issues brought up by the facts of the case, like financial advantages or losses avoided because of the infringement.

"The General Data Protection Regulation" (GDPR) of the European Union is meant to apply to all types of businesses, from small start-ups to global conglomerates. Article 83 fines under the GDPR are scalable and rise in direct proportion to the firm. Any organisation, no matter how big or small, that violates the GDPR is subject to serious consequences.

GDPR prescribed two types of sanctions for different categories of Data Infringement.

Type A: A fine of up to €10 million, or 2% of the company's global annual revenue from the previous fiscal year, whichever is higher, could be imposed for less serious infractions. This

fine is imposed if the data fiduciaries are found in violation of Articles 8, 11, 25-39, 42, and 43, (Organizations that collect and control data (controllers) and those that are contracted to process data (processors) must adhere to rules governing "Data Protection", lawful basis for processing, and more. As an organization, these are the articles you need to read and adhere to.)[107], Articles 42 and 43 (Accredited bodies charged with certifying organizations must execute their evaluations and assessments without bias and via a transparent process) and Article 41(Bodies that have been designated to have the appropriate level of expertise must demonstrate independence and follow established procedure in handling complaints or reported infringements in an impartial and transparent manner).

Type B: The more flagrant infractions go against the core principles of the GDPR, which include the right to "Privacy" and the "Right to be forgotten". For these kinds of infractions, the corporation may be fined up to €20 million, which is equivalent to 4% of its global yearly revenue from the preceding fiscal year. These include any violations of Articles 5, 6, and 9, which mandate that data fiduciaries process client data in a way that is compliant with the law. According to Article 7, an organization must have the necessary records to support its claims that processing data on an individual is justified based on that person's consent. According to "Articles 12–22", people have a right to know what data an organization is collecting and how it plans to use it. In addition, they are entitled to a copy of the information that was collected, to have it updated, and in certain cases, to have it removed. People also have the right to have their data transferred to another organization. According to Articles 44–49, the data fiduciary must guarantee the same level of data security as is offered to customers under GDPR if any amount of data is transferred to a third nation.

[107] What are the GDPR Fines?, GDPR.EU (2018), https://gdpr.eu/fines/ (last visited Oct 27, 2023).

Indian Perspective: In India, the exchange or receipt of personal information in oral, written, or electronic form is not protected by separate regulation. The most important clauses are found in the "**Digital Personal Data Protection Act (2023)"**, "**IT (Amendment Act of 2008)" and the "IT (Sensitive Personal Data or Information) Rules of 2011"**. The very first draft of "Data Protection" Act came in 2018 after recommendations given by Justice B. N. Srikrishna Committee. There were plenty of negotiations over the same in the year 2019 and 2020. However, those negotiations failed eventually, thereby scrapping the 2018 "Data Protection" Act in the year 2021. This was replaced by another "Digital Personal "Data Protection" Act, 2022". It was passed in both Lower house and Upper house of parliament in second week of August, 2023 and received president's assent on 11th August, 2023. It has now officially become law of the land, holding the title of "Digital Personal "Data Protection" Act, 2023"[108]. The chronology shows that Indian administration has put forth concerted efforts to protect personal information of its citizen that are in digital domain. It is now an even more challenging task to act as a protector and restrict the perpetrators. As per the objective of Digital Personal "Data Protection" Act, 2023 (hereinafter referred to as "DPDP Act"), this legislation is designed to regulate the handling of digital personal information, by acknowledging the importance of safeguarding individuals' personal data while also permitting its lawful processing and related issues. Major participants of this legislation are "Data Fiduciary", "Data Principal" and ""Data Protection" Officer". Data fiduciary will determine the method and reasons for using or processing personal data. Generally, the government or persons authorized by government plays the part of data fiduciary. Data principal is the one whose personal data is being used or processed by authority, such as a common person or a legal person for that matter. At this juncture, a

[108] Digital Personal "Data Protection" Act 2023.pdf, https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf (last visited Oct 27, 2023).

question arises as to what exactly will account as "personal data". It has been vaguely defined as 'any data' about the individual. There is no doubt that Indian parliament has done a commendable job by bringing and implementing this legislation, but we might have to dig deeper to understand the loopholes that have been left open, to have a stronghold of government in power. In this segment, authors have cut to the chase and tried to address the elephant in the room. A large group of thinkers object the very usage of "DPDP Act". When ruling government has been provided the supreme power to protect its subjects, it must not use it for its own advantage. We have come across various ambiguous clauses that provide wide ranging surveillance power to the authority. It seems not the data fiduciary or data processor, but the data principal is under the radar. To begin with, we will first go through the Section 2 – the definition clause. These definitions appear to establish a foundational framework for data "Privacy" laws, yet there are some contentious points that might be frowned upon. The definitions of "data fiduciary"[109] and "significant data fiduciary"[110] are very broad. These terms may be interpreted to mean that they include a wide range of organizations and give the government greater authority over different organizations. Similarly, the term "processing"[111] is broadly defined and includes a number of activities related to personal data. Such an extensive breadth provided to this term can be used to justify widespread data collection and manipulation by government agencies or their assignees, if not properly regulated.

The definition of "automation" is also very broad and includes any digital mechanism through which we can process data. This could be used to justify automated surveillance or data collection without clear boundaries. It says that all procedures can be carried out online. While this may improve efficiency, it may also solicitude the transparency and accountability

[109] *Id.*
[110] *Id.*
[111] *Id.* Section 2(x) Digital Personal "Data Protection" Act, 2023, pg.3.

matters, particularly if online procedures lack adequate oversight. There must be a proper mechanism to make those working behind the screens in digital office accountable. Lastly the term - "Certain Legitimate uses"[112]. Although this term is thoroughly discussed in later provisions of "DPDP Act", yet its interpretation and practical application can give rise to various underlying disputes. What is considered "legitimate use" varies, and this can be exploited. Under the definition segment reference has been made to section 7. Now, section 7 has some chilling clauses through which government is eligible to use data for any of the purposes, under the garb of sovereignty, integrity and "security of India"[113]. While there is nothing wrong in protecting the sovereignty and integrity of our country, but it also gives immense power to those in authority to frame an innocent as a threat, manipulating his or her digital personal data. We have seen such cases in the past[114]. These open-ended clauses bring us back to square one of individual hardships against government's authoritarian role-plays. Nonetheless, the language of "DPDP Act" is quite simple and easy, yet some sections are loaded with draconian measures in plain sight. Section 4[115] talks about the grounds of processing personal data. According to the first ground, processing any of the data will need the data fiduciary's consent. The second justification, though, is "for certain legitimate uses." This implies that any personal data may be used for any legitimate purpose, even in the absence of the subject's agreement. The unclear aspects surrounding "certain legitimate uses"—also known as legal purposes—have previously been covered in previous discussions. Ascertaining all the contentious issues related to "DPDP Act", it is pertinent to note that no matter how weak or strong this legislation is, India needed one. Undoubtedly, we have come across certain flaws, but they can easily get resolved later through robust checks and

[112] *Id.* Section 2(d) Digital Personal "Data Protection" Act, 2023, pg.2.
[113] *Id.* ection 7 (c) Digital Personal "Data Protection" Act, 2023, pg.2.
[114] *Nastasi, G. (2020). Where Victims of "Data Breach" Stand: Why the Breach of Personally Identifying Information Should Be Federally Codified as Sufficient Standing for "Data Breach" Causes of Action. Cardozo Arts & Ent. LJ, 38, 257.*
[115] Digital Personal "Data Protection" Act 2023.pdf, *supra* note 11. Section 4 of Digital Personal "Data Protection" Act, 2023, pg.4.

balances, public scrutiny and judicial oversight. Any potential abuses of this legislation must be addressed through advocacy and legal actions.

Along with “DPDP Act”, the “IT act” also covers some of the loop wholes present in the “Indian Data Protection system”. Corporate entities handling sensitive personal data or information are required under the “IT act” to reimburse damages for any losses resulting from their failure to establish and maintain appropriate security policies and procedures. While the “IT act” does not define reasonable security practises and procedures,' the SPDI Rules, which are established by the “IT Act”, specify basic “Data Protection” criteria for sensitive personal data. The SPDI Rules are not meant to be thorough, but they do require enterprises to have a “Privacy” policy, acquire consent before collecting or transmitting sensitive personal data or information, and notify data subjects of the receivers of such gathered data. One of the key contrasts between the SPDI Rules and other more current data regimes is that consent remains the essential basis for data processing. In this regard, the “IT act” also imposes criminal penalties, including up to three years in prison and fines, for those who disclose personal information without the consent of the person to whom the data relates, where such disclosure violates a contract or results in wrongful loss or gain. Thereafter SPDI standards were adopted as part of the “IT act” with the goal of protecting other sensitive information such as passwords, financial information, physical, physiological, and mental health issues, sexual orientation, medical records and history, and biometric information. However, this particular regulation was totally dependent upon ‘Consent’ based permission policy. It should be mentioned that, in contrast to “Data Protection” policies, the meaning of consent is still not fully established. As of right now, the “Indian Contract Act” defines "consent." As a result, the SPDI rules' loophole still has to be addressed. All applicable laws and regulations pertaining to the IT Act, 2000 were lacking the safeguards and restrictions necessary to secure sensitive personal information submitted online when

they were originally put into effect on October 17, 2000. This led to the introduction of the “Information Technology Act 2006” and the subsequent “IT (Amendment) Act, 2008”, the provisions of which came into force on October 27, 2009. It amended Section 43A of the “IT act” to clarify that if "a corporate body possesses or deals with any sensitive personal data or information, and is negligent in maintaining reasonable security to protect such Data or information, which thereby causes wrongful loss or wrongful gain to any person, then such corporate body shall be liable to pay damages to the person(s) so affected." Also included is Section 72A, which states that “the punishment for disclosure of information in breach of Lawful contract and any person may be punished with imprisonment for a term not exceeding three years, or with a fine not exceeding up to five lakh rupees, or with both, in case disclosure of the information is made in breach of Lawful contract”. “Section 72” specifies the punishment. It states that "any person who, in pursuance of any of the powers conferred under the “IT 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 punishable with imprisonment for a term which may extend to one year." Anybody who breaks the law or commits an offense outside of India is subject to the same penalties as someone who does so within the country, as stated in Section 75 of the Act. The “IT act”and Rules, however, have a narrow scope and breadth. Most regulations are limited to "sensitive personal data and information" obtained through the use of "computer resources." Only a limited portion of the restrictions are enforceable by consumers, and the rules only apply to companies that use automated data processing. Data localization is not addressed is the main worry and the basis for the Indian government's decision to ban Chinese applications. India needs robust data “Privacy” legislation to address these limitations.

Draft legislation and policies:

The following draft laws and policies that regulate “Data Protection” principles are at various stages of discussion or implementation:

- Non-Personal Data Governance Framework ('the NPD Framework'), which is currently being deliberated by the Committee of Experts constituted under the Ministry of Electronics and Information ('MeitY'), whose reports on non-personal data can be accessed here and here;
- Draft National Data Governance Framework Policy;
- Digital Information Security in Healthcare Act, 2017 ('DISHA');
- Framework for the India Digital Ecosystem Architecture 2.0, which is a consultation draft released by Centre for Development of Advanced Computing under MeitY; and
- Ayushman Bharat Digital Mission ('ABDM') and the draft revised Health Data Management Policy issued by the Ministry of Health and Family Welfare.

Indian courts have determined that it falls under Article 21's provision of the right to life. However, there has always been some ambiguity over the precise nature of the constitutional protection of “Privacy” because of the Supreme Court's long-standing ruling in “Kharak Singh v State of Uttar Pradesh”, which held that a right to “Privacy” did not exist under the constitution. It became vital to resolve this misunderstanding due to two factors that got more and more relevant when the government implemented its project for unique biometric identity (Aadhaar) and global events that were happening at the same time. The credit for a setting up an enriched Digital services sector in India can given to the ever growing information technology sector as well as the telecom revolution that started in the late 1990s. There have

been two main effects of this. 1st, the growth of digital platforms and services has increased national connectivity. 2nd, the government has acknowledged that achieving policy objectives like cash transfers and financial inclusion may be achieved through the appropriate use of online service delivery. The implementation of Aadhaar has significantly benefited the second purpose. However, there has been a lot of criticism directed against Aadhaar's increasing prevalence. One criticism was that Aadhaar was being used for things other than delivering societal benefits, such enrolling clients for private firms. It was argued that keeping consumer data connected to Aadhaar, including metadata about the authentication site, amounted to a serious invasion of "Privacy". The government's ability to carry out far more invasive monitoring will be made possible by the widespread implementation of Aadhaar, which was another key cause of dispute. Concurrently, to harmonize and consolidate its previous "Data Protection" framework, the European Union (EU) introduced the General "Data Protection" Regulation (GDPR) in 2013. The European "Data Protection" Directive of 1995 served as the foundation for the previous framework, which protected personal data. There was concern that this legislative structure would lead to a disjointed "Data Protection" law within the European Union. The GDPR was the subject of lengthy consultations before to going into effect in 2018. The EU's effort to create a thorough "Data Protection" regulation has also fuelled discussion in India.[116].

Aadhaar's "Privacy" concerns gave rise to a disagreement that led to numerous challenges being filed before the Supreme Court, questioning the constitutionality of the "Aadhaar Targeted Delivery of Financial and Other Subsidies Benefits and Services Act" 2016, the legislation that authorized the system. The five-judge Supreme Court bench considering the petitions declared that, in light of the claims made in the petitions, it was first imperative to determine whether the right to "Privacy" was guaranteed by the constitution. First, it was

[116] FUNDAMENTAL TEXTS ON EUROPEAN PRIVATE LAW, *supra* note 20.

important to determine whether the constitution guaranteed this right. It brought the case to a nine-judge Supreme Court bench, which decided in August 2017 that "Article 21" guaranteed a right to "Privacy", that the Supreme Court had erred in its "Kharak Singh" decision, and that this right included informational "Privacy". In the meanwhile, the government established a committee in July 2017 to investigate "Data Protection" concerns and suggest legislation in response to calls for comprehensive "Data Protection" laws. The committee, led by Justice B.N. Srikrishna, released a draft "Personal Data Protection" Act, 2018 along with a report detailing the rationale for a "Data Protection" legislative framework. [117]. The "Asia-Pacific Economic Cooperation (APEC)" "Privacy" Framework and the GDPR, two established frameworks for protecting "Privacy" in other nations, serve as a major source of inspiration for this policy. These guidelines are based on earlier "Privacy" protection regimes from the 1970s. A 1973 report from the US Department of Health, Education, and Welfare offered a set of guidelines that have since been adopted by "Privacy" laws in numerous other nations. In reaction to the fast technological advancements of the 1970s, particularly computerization and automated processing by government and private businesses, the "Records, Computers, and the Rights of Citizens" report was published. After that, organizations like the Organization for Economic Cooperation and Development adopted the report's main recommendations, which included prohibiting the gathering of data without authorization, limiting its use, ensuring data processing was transparent, and granting individuals the right to have their data corrected[118].

The reader is undoubtedly going to wonder if these late-1970s policies are still applicable now. The answer to this is that the internet and all other modern tech giants were either

[117] PIL-Thesis-2022.pdf, https://www.duo.uio.no/bitstream/handle/10852/97687/1/PIL-Thesis-2022.pdf (last visited Jun 10, 2023).
[118] ACT WHYMAN, *Secrets From Cloud Computing's First Stage: An Action Agenda for Government and Industry*, (2021), https://itif.org/publications/2021/06/01/secrets-cloud-computings-first-stage-action-agenda-government-and-industry/ (last visited Jun 10, 2023).

nonexistent or only in their infancy in the late 1970s and early 1980s. At that time, state governments owned the most of the data. Today, we may even store important consumer data on our home computers, and if the government is permitted to control the majority of the data, it would turn the country into a police state like to China. As a result, we require a more democratic structure that can withstand the demand of protecting individual "Privacy" in the face of a BIG DATA ecosystem controlled by AI.

Features of "DPDP Act":

A legislative framework for the collection and use of personally identifiable information is established by the Act. The Act suggests creating a "DPA" to create regulations and uphold the legal framework, in addition to defining a set of rights and obligations for the handling of personal data. Additionally, the measure assigns the "DPA" the responsibility of enforcing the substantive standard-setting powers granted to the federal government.

1. The Act's broad scope of applicability is an essential aspect. it applies to all businesses in India save those specifically exempted. This would cover any business that collects data through automated techniques. (The "DPA" will have the authority to classify small companies based on turnover, the volume of data handled, and data collecting reasons[119].) This would cover not just tech companies and online retailers, but also real estate companies and brokers, bank business correspondents, car dealers, lodging establishments, and dining establishments. (The GDPR affects 23 million small businesses in the European Union.)
2. The Act places consent at the centre of the suggested framework for "Data Protection". It recommends that only explicit, voluntary, and free consent—along with a means for withdrawing that consent—be used to process personal data. Any

[119] 373_2019_LS_Eng.pdf, http://164.100.47.4/ActsTexts/LSActTexts/Asintroduced/373_2019_LS_Eng.pdf (last visited Jun 10, 2023).

processing of data without this kind of consent is prohibited and may be subject to penalties. The law distinguishes between "sensitive personal data" and states that processing of that type of data requires "explicit consent." After giving the user (referred to as the "data principal") sufficient information about the kinds of data that will be collected and the purposes for which they will be gathered, consent must be obtained. It is also required to notify users and data collectors (who are legally referred to as data fiduciaries) of their rights and responsibilities. Certain situations are excluded from the Act's notice and permission requirements. These situations include carrying out legally authorized state operations, offering medical or health services in times of emergency or pandemic, and offering services in the event of a disaster or "breakdown of public order." The guidelines also contain exceptions for employment-related purposes.

3. The data holders are in charge of making sure the information is accurate and kept for as long as is required to accomplish the goals of data collecting. It will also be responsible for fulfilling any Act compliance obligations. There are further restrictions on the usage and storage of data. In accordance with the Act's “Right to be forgotten”, a consumer may request that a data fiduciary "restrict or prevent the continuing disclosure of personal data"; grant access to specific personal data in "a structured, commonly used, and machine-readable format"; allow the data to be transferred "to any other data fiduciary" (right to data portability); and correct inaccurate data (right to correction and erasure).
4. In addition, data administrators have to create grievance-redress systems, adhere to transparency requirements, implement “Privacy” by design (i.e., business practices that anticipate, identify, and prevent harm to consumers), and create security safeguards like encryption and techniques for de-identifying personal data. There are

extra obligations for "significant data custodians". Prior to processing sensitive personal data, they have to consider the implications, maintain documentation of "important operations in the data life-cycle," audit their data processing policies and procedures, and hire “Data Protection” officers.

5. The Act exempts some forms of data collection and processing from certain requirements. It states clearly that "any agency of the government" may be excluded from "all or any provisions" by the central government through the issuance of an appropriate order. Moreover, where data is handled for “domestic or journalistic, statistical or legal or investigative or research purposes”, certain provisions of the Act will not be applicable. Moreover, it recommends restricted exclusions for "manual processing by small entities."
6. The Act creates an increasing framework for data processing and storage based on the sensitivity of the data and mandates that data fiduciaries store specific data in India (data localization). It provides three types of data: important personal data, sensitive personal data, and personal data with its own set of localization requirements. Personal information is freely shared. Under the measure, users' express consent and previous government authorization are prerequisites for the transmission of sensitive personal data outside the nation for processing purposes only.
7. Penalty- If data fiduciaries fail to comply with specific provisions, monetary fines are contemplated. These can be as much as "4% of the total worldwide turnover of the Company" or 150 million Indian rupees ($2.1 million), whichever is greater. Finally, the measure proposes criminalizing actions that result in the re-identification of individuals. This offense is cognizable, which means it can be arrested without a warrant and is non-bail able.

Comparative Analysis:

Major requirements under the GDPR	Major Compliance Provisions under DPDP
1. Review and update current "Privacy" and "Data Protection" policies to ensure GDPR compliance. 1.A Create and implement employee training on "Data Protection", the GDPR, and data subjects' rights and freedoms.	1. Failure to bring internal policies in line with the legislation could result in fines under S. 27,33, 37, 42 and under Schedule 1 .
2. Implement appropriate processes for obtaining and verifying consent from data subjects, reflecting the raised consent conditions.	2. S. 6 requires that consent should be voluntary, informed, unequivocal, and specific.
3. Decide how to collect and store proof of elevated consent.	3. Section 6(1) requires that "...the data principal's explicit consent to the processing of any sensitive personal data be obtained."
4. Create "a method of withdrawing consent that is as easy as giving consent."	4. Section 6. (2) requires data fiduciaries to ensure that consumers/data principals have the right to withdraw consent after providing it.

5. Create capabilities for responding to data subjects' requests for data access.	5. Section 11 (1) provides a right of access.
6. Inform users of their "right to object to processing, as well as rectification and erasure rights."	6. Section 12 guarantees the "right to correction and erasure." **No acknowledgement of "Right to be forgotten"**
7. Responding to requests for data portability in an acceptable digital format, and when necessary, delivering the needed data directly to the new provider.	7. Section 16 guarantees protection of processing personal data without the consent.
8. Examine the notion of "Data Protection" by design and default in comparison to... existing systems and processes."	8. No **'"Privacy" by Design'** Policy under the new Law.
9. Document all data processes and align them with "GDPR requirements." Maintain detailed records of all data processing processes.	9. Essential for both general compliance and particular requirements, such as those pertaining to purpose limitation under S. 5, collection limitation under S. 6, and fair and reasonable processing under S. 4.
10. Appointment of a "Data Protection" officer is required under GDPR Norms.	11. Section 2(l) defines "Data Protection" officer, and section 18 requires appoint of a "Data Protection" Board by the central government.

11. Examine data processing and sharing agreements with other firms and determine whether they adhere to GDPR regulations. 11.A Analyze the effectiveness of the organizational and technological security measures that third parties have implemented to protect personal information. 11.B Create or adopt certification systems or rules of behaviour to manage third-party "Data Protection".	11. Section 6 holds the "data fiduciary accountable for any processing undertaken by it or on its behalf it is done without the consent of the customer".
12. Conduct an end-to-end data inventory and audit to identify all locations where personal and sensitive personal data is stored, processed, or sent.	12. Section 10(2) requires important data fiduciaries to conduct data audits.
13. Monitor "data flows to and from countries outside the European Union taking into account the legality of such transfers under GDPR".	13. Section 16 governs cross-border transfers of personal information. This requirement will apply to any companies that send data outside of India.
14. Identify organisational and technical methods that make personal and sensitive personal data inaccessible to the organisation to preserve data	14. Section 8(5) requires data fiduciaries to create security safeguards

subjects' rights and freedoms. Implement "identity management and access control" to ensure that only the appropriate persons have access to data at the appropriate time.	
15. Keep detailed records of the organisational and technological measures that have been examined and implemented, and ensure that you can “demonstrate actions and mitigations aligned with GDPR compliance” when audited or monitored by a supervisory authority.	15. S. 11 empowers the “Data Protection” Authority to monitor all “Data Protection” measures implemented by data fiduciaries.
16. Determine the legal basis for each type of data maintained and the accompanying processing performed on such data.	16. Processing may take place on the basis of permission under Section 11, or on one of the grounds listed in Sections 12-14. The foundation for such processing must be developed.
17. Establish appropriate practises for verifying data subjects' age and, where necessary, obtaining parental or guardian consent for services directly targeted at	17. Section 9 governs the collecting of personal information about children.

children.	
18. Put in place proper procedures and notification systems that will be activated in the case of a “Data Breach”.	18. “Section 8(6)” requires data fiduciaries to notify the “DPA” of “Data Breach”es "where such breach is likely to cause harm to any data principal" and to take corrective action.
19. Create automated tools for discovering, cataloguing, and categorizing personal and sensitive personal data throughout the organization.	20. The Act also differentiates between personal data and sensitive personal data, with separate compliance obligations for each.

Impact of the DPDP Act on Indian Economy:

This Act must protect personal information in a way that protects “Privacy” and fosters innovation and economic development. The majority of people in India “have only recently been able to use the internet”. Compared to people who are already accustomed to living in a digital ecosystem, digital connectivity empowers a segment of the population in a nation with inadequate electrical, transportation, and communication infrastructure very differently. The legislation will therefore have a significant economic impact. At the moment, India is home to a limited number of globally and nationally recognized IT enterprises, as well as massive e-commerce and fintech companies vying for customers. However, the vast majority of businesses are tiny. "Of the expected number of 633.92 lakh firms, just 4000 were significant and therefore out of the MSME

sector," according to the most current annual report from the Ministry of Micro, Small, and Medium firms." The great majority of businesses, most of whom are small businesses, will be impacted by the proposal.

The Act allows small businesses to avoid the application of numerous "Data Protection" laws. However, a business can be exempted only if it processes data manually and meets other "DPA" requirements. As a result, a large number of businesses will be required to comply with the Act's standards. "Micro, Small, and Medium Enterprises (MSMEs)" have made major contributions to the expansion of entrepreneurial endeavours through commercial innovations. MSMEs are expanding their domain across sectors of the economy, generating a diversified range of products and services to fulfil domestic and global market demands. MSMEs in India play an important role by creating large employment opportunities at a lower capital cost than large industries, as well as industrializing rural and backward areas, reducing regional imbalances, and ensuring a more equitable distribution of national wealth and income.

According to the "Ministry of Micro, Small, and Medium Enterprises" annual report, a micro-enterprise in the services sector has an annual turnover of more than 1 million Indian rupees ($15,000)[120]. In 2017-2018, the majority of businesses in India were categorized as micro-enterprises[121]. However, because enterprises must manually handle data, some of these will be unable to make use of the exemptions.

Many small firms collect and process personal information as a by-product of their core activity. As a result, compliance costs for such small businesses would skyrocket. Even though the Act exempts many organisations from some of the most onerous compliance requirements, they would still be required to comply with other obligations such as notice

[120] Annual-Report-FY-2022-23-DoC.pdf, https://commerce.gov.in/wp-content/uploads/2023/03/Annual-Report-FY-2022-23-DoC.pdf (last visited Jun 11, 2023).
[121] Mehak et al., *supra* note 28.

and consent, data localization, the right to access, and individual data correction. Larger and more organised businesses, particularly in the financial and telecommunications sectors, are already subject to data security and confidentiality obligations imposed by regulators. While such organizations' compliance costs would rise as well, the size of the spike would be smaller than that of small businesses facing major compliance requirements related to data processing for the first time.

The Act's overarching preventive structure will result in large costs for Indian enterprises, according to an analysis of the principal concerns that could result in such expenses. Furthermore, in the lack of an appropriate compensation structure, the proposal to expropriate nonpersonal data is likely to be contested as an unconstitutional taking of private property, which would have a major detrimental effect on long-term incentives for innovation. The harm provisions are not specifically defined and have the potential to affect the way data-related services are regulated.

The New-Found "Privacy" and Role of State:

The "Digital Personal Data Protection" Act significantly increases the state's ability to regulate the behavior of businesses that collect personal data while also allowing the Indian government to allow any government agency to opt out of complying with the Act's requirements. As a result, "Privacy" legislation can dramatically impair "Privacy" concerns, creating a paradox. The measure intends to give the government extensive authority over "Privacy" legislation. For example, the government will have the authority to establish rules for additional categories of sensitive personal data as well as voluntary identification measures that social media businesses must implement. Furthermore, its authority to exempt any government agency from the provisions of the legislation might erode existing safeguards against government spying. Currently, government surveillance

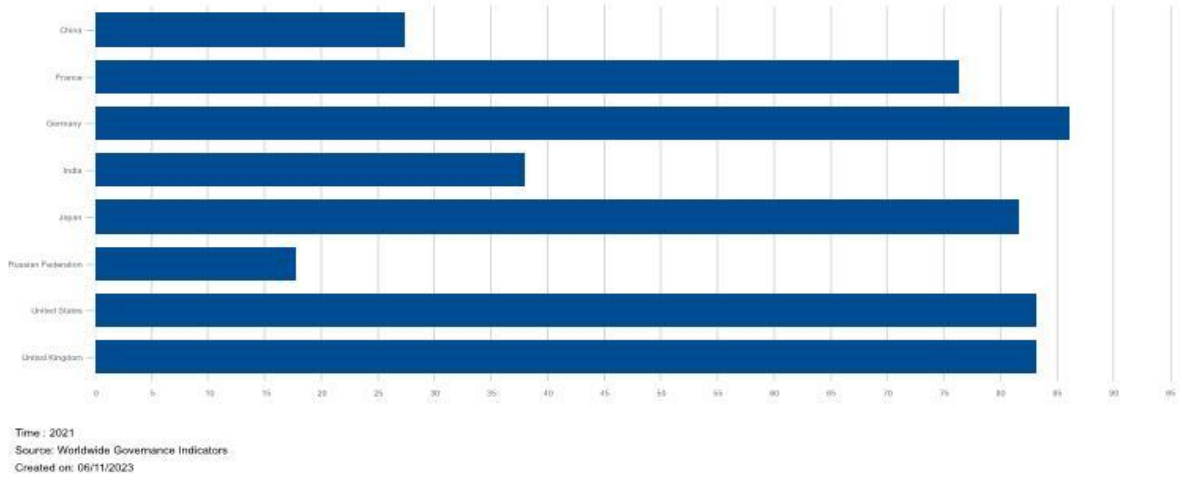
must follow the procedures outlined in the “Telegraph Act of 1885” or the “Information Technology Act of 2000”. However, under the measure, the government will have the authority to create rules governing “such procedure, safeguards, and oversight mechanism to be followed by the agency”. This creates an independent source of power to develop surveillance laws and allows the government to potentially create various safeguards for different agencies

The measure also divides the regulation of online enterprises between the government and the “DPA”, which makes sense when the nature of the regulatory authorities granted to each is reviewed. The government, for example, has substantive regulatory authority to control social media intermediaries and order them to incorporate identity verification systems. They will be considered important data fiduciaries and must register with the “DPA”. It is unclear what “Privacy” issues are being addressed by these safeguards. Identity verification may have the opposite effect—it may jeopardise the internet's premise of anonymity

Wide power to “DPA”- The act grants the authority broad powers to enforce many of the duties outlined. The “DPA”, for example, will have the authority to regulate large data fiduciaries, monitor cross-border data transfers, and devise systems for calculating "data trust scores." The law proposes that the “DPA” be given the authority to create regulations, issue directives, gather information, and conduct investigations to carry out its tasks. The Act also grants the authority additional powers, such as the capacity to write regulations and create codes of practise on topics such as notice requirements, personal data quality, consent methods, portability, transparency, and security requirements, and cross-border transfers. Such codes of practise must be prescribed by regulation or by the approval of codes of practise provided by industry organisations, statutory authorities, or government agencies. The “DPA” can only utilise these powers after consulting with

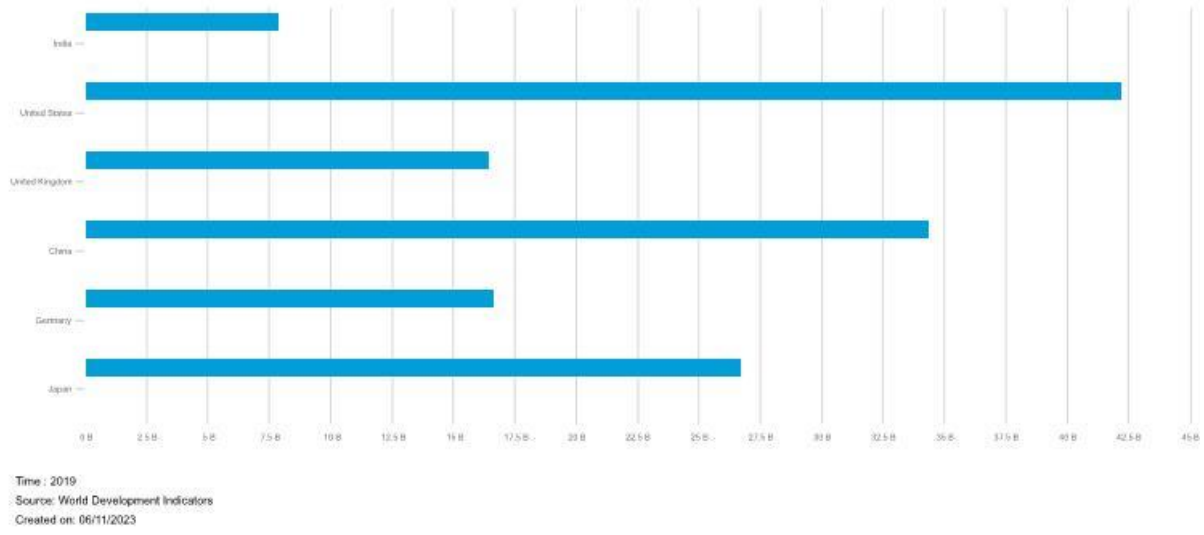
sectoral regulators and other stakeholders in accordance with the central government's guidelines. To enforce the regulations, the authority will have the right to request information and investigate any behaviour that "is detrimental to the interests of data principals," as well as impose penalties. It will also have the authority to search offices and other locations, as well as seize documents and other information.

Finding the Balance: The vast functions and powers granted to the government and the “DPA” add significantly to the state's ability to control online behaviour and commercial practises that collect user data. On the one hand, the government and the “DPA” are obligated to maintain a high level of preventative requirements for data “Privacy”, and on the other, to remedy harms and disputes through a wide range of regulatory powers. This is expected to result in two important issues: identifying priorities for regulation and capacity building, and exercising authorities in accordance with the “rule of law”. Let’s have a quick look at the **world-wide regulatory quality ranking among Asian and European Countries for the year 2021** through Figure 1. In Figure 1 I have only collected global regulatory data provided by different stake holders for the year 2021. Thereafter I have collected data regarding GDP growth for the financial year of 2019,2020,2021 and have kept A. Charges for the use of Intellectual property, B. Communication, data and computer technology export and import data as variables, which will show the GDP growth in those above-mentioned categories through Figure No.2, Figure No 3 and Figure No.4.



[122]

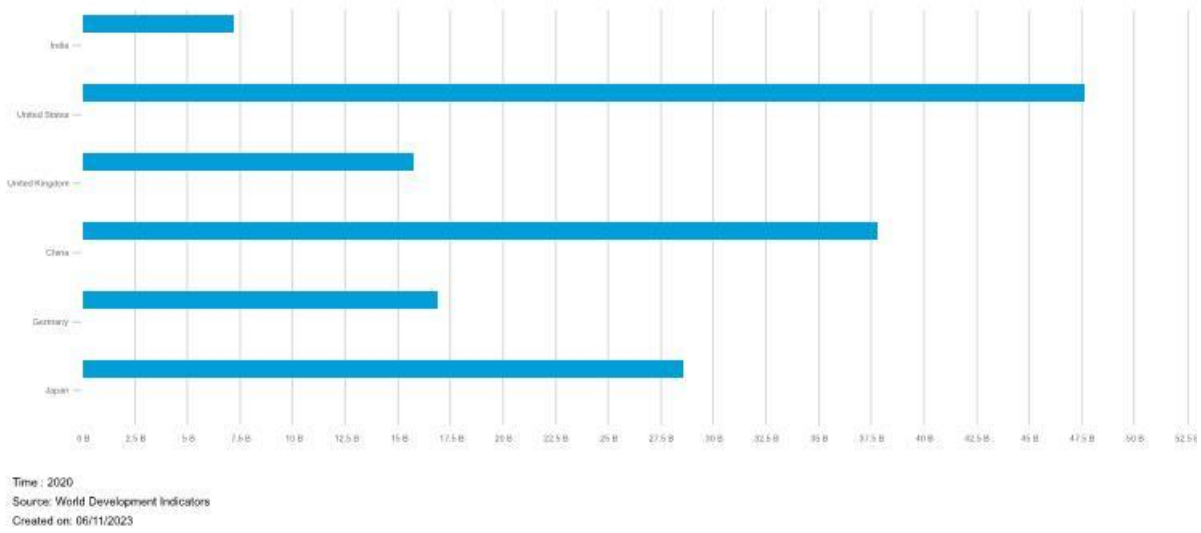
FIGURE 1



[123]

Figure 2 (For the year 2019, variable Charges for the use of Intellectual property, Communication, data and computer technology export and import data as variables)

[122] Worldwide Governance Indicators | DataBank, https://databank.worldbank.org/source/worldwide-governance-indicators/Series/RQ.PER.RNK.LOWER# (last visited Jun 11, 2023).
[123] *Id.*



124

Figure 4 (For the year 2020, variable Charges for the use of Intellectual property, Communication, data and computer technology export and import data as variables)

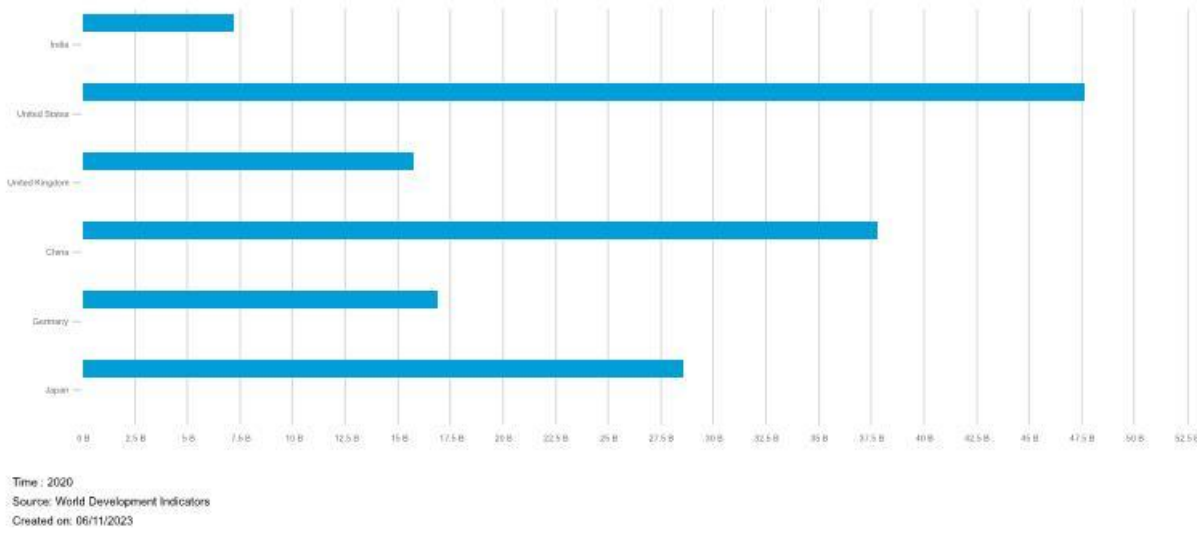


Figure 5(For the year 2021, variable Charges for the use of Intellectual property, Communication, data and computer technology export and import data as variables)

[124] *Id.*

Challenges of Regulating Data:

The nature of data itself poses challenges to data regulation. Data are limitless, and the amount of data generated by internet activity is increasing at an exponential rate. Furthermore, as technology advances, the uses of data are continuously expanding[125]. This causes issues for regulators. How do regulatory bodies effectively prevent and rectify harms in a sector as broad as "Data Protection" if the quantity and uses of data are rising at such a rapid pace? Given India's limited regulatory capacity, this concern is especially pertinent. This issue is highlighted in Figure 1, which is based on a comparison of regulatory quality across several jurisdictions. India falls behind numerous other countries with "Data Protection" regulations in place, including France, Germany, and the United Kingdom. Given the broad scope of its mission under the law and the state's overall low regulatory quality, the "DPA"'s operation is likely to be significantly hampered.

To carry out its mandate, the "DPA" and the government must prioritize their objectives. The authority must create a code of practice mandating security measures to prevent specific harms, including "Data Breach"es, and monitor compliance to prevent future harms. It also needs to provide remedies in the case that harms occur. Owing to the "DPA"'s limited capacity, a variety of factors, such as cost-effectiveness, ease of implementation, and compliance costs for regulated enterprises, are likely to influence the regulatory strategy towards focusing on one or the other.

The massive amount of data being produced, the quick speed of innovation, and the emergence of new threats along with it, along with the "DPA"'s cross-sectoral mandate, make selecting the best course of action essentially difficult. For example, the authority

[125] David Reinsel, John Gantz & John Rydning, *The Digitization of the World from Edge to Core* (2018).

will have to set guidelines for anonymization and de-identification techniques and decide whether or not these needs are being met. Both of these tasks are difficult by nature, given the speed and type of advances in data processing. Given the rapid emergence of new techniques for anonymization and re-identification, the "DPA" will require a high degree of complexity and ability to assess what qualifies as anonymization and de-identification..

Due to their relatively narrow scope of authority, sectoral regulators do not deal with an issue of this magnitude. For instance, communications authorities strictly regulate entities within their stated domain, while banking regulators regulate banking entities and intermediaries. Their significantly closer ties to particular markets enable them to develop regulatory plans with better data and in a more focused area. However, the "DPA" will oversee the security of data across numerous industries without having a thorough understanding of the unique circumstances of any of them and it will have to do so in a nation with a historically poor track record of effective regulation. There is term called 'Isomorphic mimicry' coined by Lant Pritchett, Matt Andrews, and Michael Woolcock which denotes as "combination of capability failure while maintaining at least the appearance and often the legitimacy and benefits of capability as successful failure"[126]. Alternately, the "DPA" can decide to demonstrate its efficacy by using its authority harshly. It may decide to enforce the law aggressively rather than effectively given the extensive array of regulatory measures at its disposal and the high ceilings on monetary penalties.

[126] Matt Andrews, Lant Pritchett & Michael Woolcock, *Looking like a State: The Seduction of Isomorphic Mimicry*, *in* BUILDING STATE CAPABILITY: EVIDENCE, ANALYSIS, ACTION 0 (Matt Andrews, Lant Pritchett, & Michael Woolcock eds., 2017), https://doi.org/10.1093/acprof:oso/9780198747482.003.0003 (last visited Jun 12, 2023).

Proper use of authority by the "DPA" (Digital Personal "Data Protection" act) and the government:

New and significant legal requirements (such the designation of new categories of sensitive personal data and valid reasons for data processing) may be established by the "DPA". It will also have the power to establish legislative requirements (including procedures for confirming age and consent, notification and consent forms, and measures to guarantee transparency and accountability in "Data Protection") and to impose penalties for breaking the law. The institutional framework must ensure that the "DPA" acts in a clear, deliberate manner without abusing its discretion, given its wide range of authorities and responsibilities. That being said, this is not guaranteed under the proposed legal system. Let's quickly examine the loop wholes :

1. First of all, there are no independent members included in the authority's board's proposed structure and layout. To give independent input and oversight in the operation of a "DPA", the majority of regulators in India and throughout the world have at least some independent members.
2. Secondly, the "DPA"'s and the government's ability to enact regulations is not sufficiently checked and balanced. The law requires consultation before codes of practice are published, but it does not specify what measures the "DPA" must take to have these discussions; this is left up to the government. "The Act does" not mandate that the government follow a comparable consultation process to exercise its regulatory jurisdiction.
3. India, unlike the US, lacks a general administrative structure that mandates stakeholder consultation by government organisations. As a result, when creating

regulations, Indian regulatory authorities rarely contact stakeholders. A further factor is that court review of rules is typically limited to the due-process standards listed in the parent law creating the agency.

4. As a result, the “DPA” is probably going to be a regulatory body with significant capacity limitations, broad discretionary authority, and weak accountability frameworks. These shortcomings in the design might significantly increase the regulatory burden placed on businesses throughout the economy without necessarily ensuring effective information “Privacy” protection.
5. With regard to the government, certain of these issues take on greater importance. Given that the government already has these capabilities under current laws, the broad authority to exempt government institutions from the scope of this measure is very problematic. The Act increases risks to people's “Privacy” by providing a separate source of power for governmental monitoring. It's unclear what issue this capability is meant to address. However, if such exemptions are to be granted, the legislation must specifically outline the process that government organizations must follow to break the laws governing “Data Protection”.

Creating a Regulatory Framework with Greater Effectiveness:

The regulatory mandate of the government and the “DPA” is likely to be greatly reduced by switching to a regulatory approach that focuses primarily on harms resulting from contractual conditions and decreases requirements on enterprises. A reasonable choice about the thresholds for exempting small firms will also allow the “DPA” to concentrate its regulatory capabilities on a more constrained group of companies. The inherent problems with data regulation are not resolved by this strategy, but it may improve regulatory effectiveness. The

government and the "DPA" must adhere to a solid regulatory process even with this narrower area of control. The specifics of how rules and regulations are created must be contained in the Act to guarantee that they are followed.

The Pros of Mandatory Disclosure by E-Platforms:

Theoretically, e-disclosure requirements would drive up the number of people who read standard forms and shop for terms to a point where companies could no longer afford to ignore them. Mandatory website disclosure would also enable buyers to educate themselves by examining and contrasting terms at a distance from the thrill and expectation of a near future transaction. Companies in markets with intense competition would fight for a bigger market share by crafting phrases that appeal to customers. Companies in less cutthroat sectors would try to write catchy headlines to draw in as many readers as possible[127]. Customers could shop in these markets with a certain level of assurance that the terms' quality would be suitably reflected in the prices[128].

In theory, mandatory website disclosure could still encourage companies to write fair terms even if it had little effect on consumer reading. Companies might be concerned, for instance, that disclosure would allow watchdog groups to reveal offensive language[129]. Such exposure could destroy a company's reputation, which is particularly important on the internet where customer trust is essential to success, and consequently reduce the company's market share. For example, when you are willing to write a positive review regarding any products on e-platforms, they will always welcome you. However when you would want to write a critical review, they will not allow you to do so without scrutinizing it first. I say, that's the violation of my freedom of-speech. An we are all aware that Right o "Privacy" and "Freedom of

[127] Becher, *supra* note 13.
[128] Dangerous Terms: A User's Guide to EULAs, ELECTRONIC FRONTIER FOUNDATION (2005), https://www.eff.org/wp/dangerous-terms-users-guide-eulas (last visited Feb 11, 2024).
[129] Christian J. Meier-Schatz, *A Fresh Look at Business Disclosure*, 51 THE AMERICAN JOURNAL OF COMPARATIVE LAW 691 (2003).

Speech" both forms a part of Right to Life, enshrined in Article 21 of Indian Constitution. Contract law would support autonomy justifications for contract enforcement by expanding the ability to read e-standard forms. When given the chance to read and compare terms, consumers are better equipped to decide whether and with whom to enter into a contract.

Standard forms should be inexpensive to display on a website, so the obvious costs of requiring website disclosure shouldn't be too high. In actuality, businesses haven't been able to present a convincing case against the requirement up to this point[130]. Legislators shouldn't encounter insurmountable difficulties when creating regulations that effectively incorporate disclosure. If e-businesses are to be discouraged from creating strategies to hinder reading, the regulations governing mandatory website disclosure need to be explicit and comprehensive. Plain English language that is easily readable on a website's home page or via a prominently marked hyperlink may draw in more visitors than legalese which requires multiple mouse clicks[131]. Therefore, mandatory website disclosure laws must take these tactics into consideration by mandating that companies display terms on their homepages or on a page that is only accessible through a few clicks. Moreover, scroll-down windows that vanish or are too small should be prohibited by the rules.

The cost of establishing that a company did not, or did not display its terms prior to the transaction in a way required by law, would be included in the enforcement costs. Mandatory website disclosure laws might place the onus of proving the content of websites on businesses, encouraging them to maintain accurate records of their content. Currently, a lot of online businesses maintain archived copies of their website content, which include the dates of its introduction, modification, and removal. Additionally, they keep track of server logs,

[130] Juliet M Moringiello & William L Reynolds, *What's Software Got To Do with It? The ALI*, 84 TULANE LAW REVIEW.
[131] Gary M. Olson & Judith S. Olson, *Human-Computer Interaction: Psychological Aspects of the Human Use of Computing*, 54 ANNU REV PSYCHOL 491 (2003).

which show when and if a webpage was altered. Every e-business would have to comply with a system of required website disclosure. Of course, companies that are willing to commit fraud might be able to change their records, but this issue shouldn't be all that dissimilar from the difficulty of rooting out fraud in the paper contracting industry. The testimony of other website users during the disputed period, for instance, could serve as evidence to support a business's claims. By looking through their web logs, e-businesses can locate these visitors. In the online realm, we can anticipate that as technology develops quickly and as entrepreneurs take their ideas forward, new techniques for proving website content over time will also be created. For instance, don't be shocked if new websites appear to archive the common e-business models if contract law adopts mandatory website disclosure.

Standard form of E-Contract- Their mandatory Disclosure and its Risks for Economy:

More people than ever before are considering data "Privacy" to be a serious issue; some have even declared it to be a human rights one. The majority of nations have implemented consumer protection laws that control the gathering, storing, and use of data. Businesses are responsible for making sure there are no infractions. Because e-commerce is a digital business, "Privacy" policies are especially important. E-commerce "Privacy" policies ought to be transparent about the collection, storage, use, and sharing of data. This covers every detail, including phone numbers, credit card details that have been saved, past purchases, and interactions with advertisements. 75% of consumers worldwide will be subject to "Privacy" regulations by 2023[132]. This implies that to comply with legal requirements and safeguard the data of clients, staff members, and partners, e-commerce websites need to have procedures and safeguards in place.

[132] Study predicts "Privacy" laws will regulate 75% of worldwide consumers by 2023, https://iapp.org/news/a/gartner-predicts-75-of-consumers-will-fall-under-"Privacy"-laws-by-2023/ (last visited Feb 11, 2024).

E-Commerce is the focus of mandatory website disclosure, which only enforces terms that are present on a company's website before a transaction. Naturally, the terms themselves are not required to comply with this rule. With the hope that more customers will read and search for terms, or that watchdog organizations will make negative terms public, disclosure is meant to persuade companies to write reasonable terms[133].

Currently many Developed, Developing countries have developed their own e-commerce regulation to protect "Privacy" of their own citizents. Let us have a quick look at them:

- **Consumer "Privacy" Act of California (CCPA)[134].**

The most extensive data "Privacy" law enacted at the state level is the CCPA. California law requires businesses that gather personal data about their clients to provide a clear notice of the data they collect, as well as the option to have it deleted at their request. The state's first "Privacy" law, the California Online "Privacy" Protection Act (CalOPPA), is in addition to this.

- **California "Privacy" Rights Act (CPRA)[135]**

The CPRA expands upon the CCPA by granting users the ability to limit how personal information is used, update inaccurate data, and set storage time limits for specific types of information.

[133] Efthymios Constantinides, *Influencing the Online Consumer''s Behaviour: The Web Experience*, INTERNET RESEARCH (2002).
[134] California Consumer "Privacy" Act (CCPA) | State of California - Department of Justice - Office of the Attorney General, https://www.oag.ca.gov/"Privacy"/ccpa (last visited Feb 11, 2024).
[135] California "Privacy" Rights Act, WIKIPEDIA (2024), https://en.wikipedia.org/w/index.php?title=California_"Privacy"_Rights_Act&oldid=1199231267 (last visited Feb 11, 2024).

- **Virginia's Consumer "Data Protection" Act (C"DPA")[136].**

The General "Data Protection" Regulation act of the European Union and Virginia's CCPA are somewhat similar. Businesses that sell to Virginians are required to provide opt-in options for personal information.

- **Colorado "Privacy" Act (CPA)[137].**

Colorado is the third state to enact legislation pertaining to data "Privacy", drawing from earlier legislative efforts. It includes the ability to remove information, find out what data has been collected, and choose not to receive targeted advertisements.

- **New York SHIELD Act[138]**.

Laws pertaining to the security of personal information are included in the broader set of consumer protections provided by the Stop Hacks and Improve Electronic Data Security (SHIELD) Act.

- **Connecticut's law on data "Privacy"[139]**.

The law from Connecticut has taken effect on July 1, 2023, and is applicable to any organization that owns or controls personal data.

- **The GDPR of the EU[140].**

[136] Code of Virginia Code - Chapter 53. Consumer "Data Protection" Act, https://law.lis.virginia.gov/vacode/title59.1/chapter53/ (last visited Feb 11, 2024).
[137] Colorado "Privacy" Act (CPA), CONSUMER "PRIVACY" ACT, https://www.consumer"Privacy"act.com/colorado-"Privacy"-act-cpa/ (last visited Feb 11, 2024).
[138] SHIELD Act | New York State Attorney General, https://ag.ny.gov/resources/organizations/data-breach-reporting/shield-act (last visited Feb 11, 2024).
[139] The Connecticut Data "Privacy" Act, CT.GOV - CONNECTICUT'S OFFICIAL STATE WEBSITE, https://portal.ct.gov/AG/Sections/"Privacy"/The-Connecticut-Data-"Privacy"-Act (last visited Feb 11, 2024).
[140] General "Data Protection" Regulation, WIKIPEDIA (2024), https://en.wikipedia.org/w/index.php?title=General_Data_Protection_Regulation&oldid=1203651507 (last visited Feb 11, 2024).

- The majority of current data "Privacy" laws are based on the GDPR. It is the most comprehensive regulation that has been passed to date and forms the basis of the majority of "Privacy" laws that have been passed since. Consent protections, rights to be notified of "Data Breach"es, and limitations on the use of data are all included.
- **The Electronic Documents and Personal Information Protection Act (PIPEDA) of Canada**[141].

Canada's "Privacy" protection legislation was actually initially passed in 2000 and has been amended several times to keep it up to date with changes in the use of data.

- **The General Law of Personal "Data Protection" in Brazil (LGPD)[142].**

According to the GDPR, Brazilian law is applicable to all Brazilian nationals, regardless of whether a business is headquartered there.

One may ask, despite having so much legislations in hand, why can't we protect our "Privacy" from potential risk of loss of "Privacy". Well, the answer to this question will be full of sarcasm. For instance, the new guidelines proposed by the NGT, where it is mentioned that upon taking necessary permission from NGT, manufacturers can establish their factories in protected forest land as well. This legislation was originally intended to protect Forest Land, however by taking advantage of the loop holes in the legislation many has bent the law in their favor. Similarly, as the data "Privacy" legislations are comparatively new to the legislators, it will take more time to create a wholesome legislation to protect "Privacy" of consumers on E-commerce websites.

[141] Office of the "Privacy" Commissioner of Canada, *The Personal Information Protection and Electronic Documents Act (PIPEDA)*, (2021), https://www.priv.gc.ca/en/"Privacy"-topics/"Privacy"-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/ (last visited Feb 11, 2024).
[142] General Personal "Data Protection" Law, WIKIPEDIA (2024), https://en.wikipedia.org/w/index.php?title=General_Personal_Data_Protection_Law&oldid=1205648883 (last visited Feb 11, 2024).

Coming back to our original discussion as previously mentioned, since watchdog organizations can publicize unjust terms, requiring website disclosure may encourage companies to write reasonable terms. The issue is that, while the threat of watchdog groups may incentivize companies to refrain from drafting outrageous terms, it might not be enough to stop them from drafting terms that would negatively impact consumers' perceptions even though they might not raise major red flags. For instance, a company that is concerned about watchdog groups might avoid including a clause requiring a customer to pay the company's legal fees and costs in any case or to arbitrate in a non-neutral forum. However, these clauses may still be unenforceable due to its unforeseen nature. However, a company may determine that the advantages of a forum-selection clause that causes inconvenience to the customer or a clause that permits an online platform to "collect certain non-personally identifiable information about a consumer's web surfing and computer usage" outweigh the costs of any negative publicity they may generate.

Mandatory website disclosure may have the unintended consequence of giving businesses a safe haven to use derogatory but appropriate language. Conditions that were previously deemed unconscionable or related may still be enforceable due to their reasonable disclosure[143]. Both procedural and substantive unconscionability are sought in the majority of cases involving unconscionability or related claims, including those involving e-commerce[144]. Procedural unconscionability refers to the circumstances surrounding the contract's formation and governs scenarios that bear similarities to duress, misrepresentation, or most importantly in this case an unfair representation of the terms. Although substantive unconscionability focuses on whether an exchange is egregiously imbalanced, contract law

[143] Comb v. Paypal, Inc., 218 F. Supp. 2d 1165 | Casetext Search + Citator, https://casetext.com/case/comb-v-paypal-inc-2 (last visited Feb 11, 2024).
[144] Robert A Hillman, *Debunking Some Myths About Unconscionability: A New Framework for U.C.C. Section 2-302*, 67 CORNELL LAW REVIEW.

typically does not assess the suitability of an exchange[145]. Many courts use a sliding scale in their unconscionability investigations, stating that "less evidence of procedural unconscionability is needed to conclude that a term is unenforceable the more substantially oppressive the contract term, and vice versa."[146]

"Privacy" Management:

The advent of Big Data and fusion centers, data security breaches, the rise of Web 2.0, rising marketing, and the expansion of monitoring technology have all exacerbated "Privacy" issues during the last decade. Policymakers in developed and developing countries have proposed and passed substantial new regulations, but the underlying approach to preserving "Privacy" has remained largely intact since the 1970s. The law currently offers people some rights that allow them to decide how to manage their data. These rights essentially include the rights to be notified, to access, and to consent to the collection, use, and disclosure of personal data. The purpose of this set of rights is to provide people control over their personal data, so that they can balance the costs and benefits of the acquisition, use, or disclosure of their information for themselves. In this era of e-consent management of "Privacy" is very important. Let us discuss what issues one individual may face during managing their consent and managing their "Privacy".

A. Analytical Problems: crucial aspects of "Privacy" management consist of notifying individuals about the data collected and used about them (notice) and allowing them to choose whether or not to accept such collection and use (option). By giving "Privacy" notices and the option to opt out of some of the forms of data collection and use indicated in the notices, entities have normalised the practise of providing notice and choice. In the United

[145] Hillman, *supra* note 9.

[146] *Armendariz v. Foundation Health Psychcare Services, Inc.*, WIKIPEDIA (2023), https://en.wikipedia.org/w/index.php?title=Armendariz_v._Foundation_Health_Psychcare_Services,_Inc.&oldid=1175138606 (last visited Feb 11, 2024).

States, the FTC has stepped in to enforce “Privacy” notifications. Since 1998, the Federal Trade Commission has maintained that breaching “Privacy” notice commitments constitutes "unfair or deceptive acts or practices in or affecting commerce" in violation of the Federal Trade Commission Act. When the FTC discovers such a breach, it has the authority to file civil cases and seek injunctive relief. The method of notification and choice has also been a focal point of “Privacy” regulation. For example, the Gramm-Leach-Bliley Act (GLBA)[147] mandates financial institutions to give clients with “Privacy” notifications and to let them to opt out of data sharing with third parties. People do not appear to be engaged in much “Privacy” management, despite their embracing of notice and choice. The vast majority of consumers do not read “Privacy” notifications on a regular basis[148]. Studies reveal that just a small fraction of individuals read other sorts of notices, such as end-user license agreements and contract boilerplate terms. Furthermore, when given the option, few people choose not to have their data collected, used, or disclosed[149]. The majority of individuals do not bother changing the default “Privacy” settings on websites.

People do not appear to be engaged in much “Privacy” management, despite their embracing of notice and choice. The vast majority of consumers do not read “Privacy” notifications on a regular basis. Studies reveal that just a small fraction of individuals read other sorts of notices, such as end-user license agreements and contract boilerplate terms. Furthermore,

147 2 Pub. L. No. 106-102, 113 Stat. 1338 (codified in scattered sections of 12 and 15 U.S.C).

148 4 See Helen Nissenbaum, “Privacy” in Context 105 (2010) (discussing a 2006 study showing that only 20% of people read “Privacy” notices "most of the time" (quoting TRUSTe & TNS, Consumers Have a False Sense of Security About Online “Privacy”: Actions Inconsistent with Attitudes, PR NEWSWIRE, http://www.prnewswire.com/news-releases/consumers-have-false-sense -of-security-about-online-”Privacy”—actions-inconsistent-with-attitudes-55969467.html (last visited Sept 29, 2023) (internal quotation marks omitted))); Fred H. Cate, The Failure of Fair Information Practice Principles, in consumer PROTECTION IN THE AGE OF THE 'INFORMATION ECONOMY' 343, 361-62 (Jane K. Winn ed., 2006); George R. Milne & Mary J. Culnan, Strategies for Reducing Online “Privacy” Risks: Why Consumers Read (or Don't Read) Online “Privacy” Notices, 18 J. INTERACTIVE MARKETING 15, 20-21 (2004) (finding that only 4.5% of respondents said they always read website “Privacy” notices and 14.1% frequently read them)

149 Omri Ben-Shahar & Carl E. Schneider, The Failure of Mandated Disclosure, 159 U. PA. L. Rev. 647, 665-78 (2011); Florencia Marotta-Wurgler, Will Increased Disclosure Help? Evaluating the Recommendations of the ALI's "Principles of the Law of Software Contracts," 78 U. chi. L. Rev. 165, 178 (2011) (discussing a study that revealed that people accessed contract boilerplate terms far less than 1% of the time).

when given the option, few people choose not to have their data collected, used, or disclosed. The majority of individuals do not bother changing the default "Privacy" settings on websites[150]. A more difficult issue occurs when ideas for improved notice, whether simplified or more obvious, are proposed. Such techniques neglect a fundamental usage of notice: keeping things simple and easy to understand clashes with thoroughly informing people about the consequences of disclosing data, which are pretty difficult to understand if presented in sufficient detail to be meaningful. People need a greater understanding and background to make informed decisions. However, many "Privacy" notices are vague about potential future data usage. Furthermore, if people wants to read and understand the terms and condition they are not usually allowed to do so. For example, if you want to unsubscribe any services online, the service provider will start redirecting you to countless subsidiary websites and make it more complex.

B. Making unreasonable decision: Even if most people read "Privacy" policies on a regular basis, they frequently lack the experience to fully assess the ramifications of agreeing to specific present uses or disclosures of personal data. People often hand out their data for insignificant rewards[151]. Some draw the conclusion that consumers place little value on "Privacy". Some argue that there is a generational shift in "Privacy" norms, with young people not caring about "Privacy". However, people consistently declare how much they value "Privacy" in surveys, and attitudes towards "Privacy" among the young and old are, unexpectedly, relatively similar[152].

[150] ee M. Ryan Calo, Against Notice Skepticism in "Privacy" (and Elsewhere), 87 NOTRE DAME L. Rev. 1027, 1033 (2012) ("Studies show only marginal improvement in consumer under standing where "Privacy" policies get expressed as tables, icons, or labels, assuming the consumer even reads them")

[151] Alessandro Acquisti & Jens Grossklags, "Privacy" and Rationality: A Survey, in "Privacy" and technologies OF Identity is, 16 (Katherine J. Strandburg & Daniela Stan Raicueds., 2006)

[152] Chris Jay Hoofnagle et al., How Different Are Young Adults from Older Adults When It Comes to Information "Privacy" Attitudes & Policies? (Aug. 14, 2010) (unpublished manuscript) available at http://papers.ssrn.com/s0l3/papers.cfmPabstract_ids 1589864

Conclusion: The Right to "Privacy" is a well celebrated right among the citizens of Urban India, however the light of this right is yet to reach the furthest corners of this country. One Might ask, what do you mean by this? In urban India most of us are well connected with the super-giant of information AKA Internet. With the growth of Information technology, the cost of connectivity has significantly gone down, and this phenomenon has given the opportunity to all and sundry to connect themselves with the social media giants like Facebook, Twitter, Instagram, Tiktok and YouTube etc. Can anyone of us tell, how many of us are actually read the user policy before installing an app or subscribing to a certain website? Studies has shown that approximately 60% of Indian users do not read the "Privacy" policy provided during the installation of any app or software in their electronic devices[153]. This data reveals that most of us Indians are not well versed with the data "Privacy" policy or are not even interested enough to read the policies. Because of such casual approach we are putting ourselves in a dangerous position of "Data Breach".

To summarize, this Chapter highlights the following major issues with the Digital Personal "Data Protection" Act:

First, it establishes important restrictions on data processing and mandates notice and consent for data acquisition. Since they are founded on concepts for the control of data (fair information practices) developed prior to the creation of the current market structure, these collectively may not truly effectively guarantee "Privacy". Additionally, they do not shield consumers from the negative effects of "Privacy" infringement. Instead, these requirements

[153] Shariq Khan, *60% Online Users Fear Unauthorised Data Collection, Only 11% Users Read "Privacy" Policies: Survey*, THE ECONOMIC TIMES, Mar. 11, 2019, https://economictimes.indiatimes.com/small-biz/policy-trends/60-online-users-fear-unauthorised-data-collection-only-11-users-read-"Privacy"-policies-survey/articleshow/68355981.cms?from=mdr (last visited Jun 4, 2023).

might raise moral hazards and cause consumers to overestimate the advantages of “Privacy” legislation.

Second, there is no empirical understanding of the trade-off’s users make when disclosing their information, hence the Act has no basis in reality. The Srikrishna committee, which created the initial draught of the Act, did not do any research to determine the particular situations in which users are willing to trade personal information for advantages. Evidence from different jurisdictions suggests that these trade-offs vary depending on the transaction's environment. If the Act effectively safeguards personal data without demonstrating its relevance to users, it may have a negative impact on the advantages of data-driven innovation.

Third, the Act wants to charge businesses that process data with high compliance expenses. Small firms are excluded from a lot of requirements; however, these exemptions only apply to companies who process data by hand. As a result, putting the measure into effect would be quite expensive for a wide range of economic actors. The regulations that force companies to give the government non-personal data are very onerous and significantly erode property rights. Long-term consequences for innovation and economic growth may result from this.

Fourth, the term "harms" is poorly defined. Many of these actions are necessary for making business decisions in general. The Act's concept of injury may drastically skew how corporations are regulated while offering no “Privacy” protection.

Fifth, The government's ability to create new, independent means of collecting personal data by allowing government institutions to operate outside the law to conduct surveillance. It is unclear why this provision is required, and the measure lacks adequate checks and balances for the use of these powers.

Last but not least, there are structural problems with the “DPDP Act”'s design. The Act's extensive preventive structure will severely limit its ability to do things. Independent inputs and oversight are not permitted by the authority's planned structure. Additionally, the DPDP might not be compelled to adhere to sufficient consultative procedures when performing its regulatory-making duties.

The effectiveness of safeguarding “Privacy” through this regulatory structure obviously has its limits. The framework should instead concentrate intently and narrowly on issues that can be meaningfully resolved by legislation. The potential elements of such a framework are listed as follows:

1. **Consent Clause:** Businesses who disregard this rule would also be violating the users' property rights and the constitutional information “Privacy” rules of India. Conscientious adults must also be given the freedom to make their own decisions. In other consumer-focused industries, regulation typically involves deciding if particular contractual provisions and business practises are unfair, deceptive, or misleading to customers. The law should emphasis on identifying and regulating such practises as well as provisions in data sharing agreements rather than imposing preventive obligations. The Act falls short in providing effective protection against specific user damages or injuries. The emphasis should be on preventing harm to people and society that results from a breach of data “Privacy”, including risks to sovereignty and national integrity, identity theft, fraud, and discrimination on legally recognised grounds. The laws on hazards must also be revised using this emphasis on injury prevention. For causing harms of the kind mentioned above, data fiduciaries should be held accountable. However, they shouldn't be compelled to take preventative action against every possible data misuse scenario. Market failures should only be the focus

of regulation. It would be necessary to abandon obligations like “Privacy” by design and the hiring of “Data Protection” officers to reorient to a narrowly tailored strategy.

2. **Regulatory obligations should be layered, based on an assessment of their costs and benefits:**

   Reduced obligations for businesses who do not handle sensitive personal data or treat data sparingly should be done in a way that is proportionate to the dangers posed by their operations. The requirement that firms manually handle data to qualify for the exemptions may be one of these reductions.

3. **Reduction in Uncertainty:** The Act's ambiguities must be kept to a minimum to increase business certainty. The law now has three key problems that could result in severe regulatory uncertainty. It does not adequately define vital personal data, to start. Second, it doesn't outline the standards for permitting data transfers across international borders. Thirdly, it grants the government the authority to enforce the sharing of non-personal data without imposing any usage restrictions or specifying how much compensation will be paid.

4. **Balance of Power:** It shouldn't be up to the government to decide which agencies receive exemptions and what protections should be in place for them.

5. **The mandate given to the “DPA” should be cognizant of state capacity constraints in India**: It will be nearly hard to adequately govern data processing given the nature of the data economy. The additional ideas presented here can rationalise the “DPA”'s mandate's reach. The authority's authority to oversee the right to access, the “Right to be forgotten”, and other rights would end. Additionally, it would not have the authority to determine how requirements like purpose limitations should be carried out. Furthermore, the “DPA” would have more guidance on how to carry out crucial aspects of the Act if the ambiguities mentioned above were removed.

Finally, raising the threshold would dramatically lower the number of companies subject to the “DPA”'s authority and allow it to concentrate on data-intensive enterprises below which firms would be exempt.

6. **Consultative process for decision-making:** Due to the cross-sectoral applicability of the regulations under the Act, this is significantly more crucial in this situation than for other regulators. Therefore, the Act should be changed to mandate that all rules, regulations, and codes of practise developed by the government should undergo a thorough consultative process with the “DPA”. A thorough consultation approach for financial industry regulators was suggested by the financial industry Legislative Reforms Commission (2013) and was included in the actual legislation. This mandated that the board or the regulator's highest decision-making body begin the regulation-making process by first publishing a draught of the proposed regulation together with a note outlining the rationale behind the proposal and an appraisal of its advantages and disadvantages. Additionally, it was suggested that prior to drafting the final regulation, each financial sector regulator should request public feedback on the draught and publish a comprehensive response.

   Among other authorities, the Indian Insolvency and Bankruptcy Board, the Airports Economic Regulatory Authority, and the Telecom Regulatory Authority of India conduct extensive consultations before establishing regulations. The “DPA” must adhere to the Act's mandated consultative procedure. This need, however, only pertains to creating codes of conduct, and the government is given the authority to specify the specifics of the consultative procedure. The particular features of such consulting mechanisms contained in the applicable law and the completeness of the consultative process followed by Indian authorities are directly related. Therefore, the

law should be changed to guarantee that the “DPA” follows best practises for creating regulations and codes of practise.

7. **Strong Structural Integrity:** Both independent, part-time workers and full-time employees should be a part of the “DPA”. Independent members shouldn't take part in daily activities of the organisation. This would make it possible for independent contributions and a structure for external agency oversight.

   All things considered, requiring website disclosure might still be the most effective way to address the issue of e-standard forms. As previously stated, alternative solutions come with a number of serious drawbacks. Furthermore, requiring website disclosure is inexpensive, supports the assertion that consumers gave their consent, and represents a symbolic win for proponents of increased equity in e-standard-form contracts. Of course, these arguments for mandatory website disclosure are only compelling if my concern about a potential legal backlash turns out to be unfounded, as the advantages of disclosure exceed the expenses of enforcing certain dubious terms.

CHAPTER 5

“Data Protection” Regulations, Policies, and Principles in Europe, and India

Introduction: In the world of Internet and E-Connectivity our virtual identity, freedom of Choice, Consumer behavior is controlled by the various service providers of Data Industry. In earlier days Newspaers and TV used to be prime source of Advertisement and informing regarding the latest inventions of Industrial Revolution. With the introduction of Internet Facebook, Instagram, Amazon, Flipkart has replaced the earlier market as well as the physical advertisement industry. Now, you don’t even have to purchase your groceries from the Market. Honestly, I don’t remember when was the last time I bought ‘Instant Noodles’ from the Market.

It's common knowledge that whenever we visit a website, we always leave digital traces behind. In other words, we provide the service provider access to our information. The data may comprise bank account information, health-related data, and personal identifying information, among other things. Since technology enables corporations to store, handle, and exploit personal data, there has been a rise in the “Privacy” concerns of e-service users concomitant with the expanding use of the Internet for service delivery. As a result, people may feel less in control of their personal information and more at danger of “Privacy” breaches. A systematic understanding of consumers' “Privacy” concerns is critical because negative user perceptions undermine service providers' reputations and may impede service delivery procedures by influencing users' trust and willingness to reveal personal information.

A cyber attack includes unauthorized attempts to gain access to computer networks or systems with the goal of stealing confidential data, causing harm, or interfering with essential

operations. Comparable to a burglar breaking into a house to steal goods or cause harm, ""Cyber Attacks"" can take on multiple identities and originate from anywhere in the world. The people who commit these crimes can be anyone, from hackers and criminal elements to government agencies. The theft of financial records, confidential company information, or personal data are possible goals of a cyberattack. Furthermore, they might have a dark agenda to cause havoc by upsetting important systems like banks, power plants, and healthcare facilities. In the modern digital world, where "Cyber Attacks" are becoming more and more common, protecting oneself and one's data becomes crucial.

Businesses can benefit greatly from "information technology" advancements as the Internet becomes a useful tool for providing electronic services, or "e-services." A large amount of data about service users is provided by e-services from both public and private sector companies, and this data is utilized to manage service delivery and enhance the service. While this may benefit both providers and users, greater personal data collecting is risky. "Privacy" concerns stemming from the sensitivity of personal information are a major issue for users these days[154]. Furthermore, a recent survey of 25 nations found that more than half of respondents were more concerned about their internet "Privacy" now than they were a year ago. These worries are only get worse [155].There are numerous circumstances that may cause users to be concerned about their "Privacy", including, but not limited to, unauthorised access, secondary use, interception of personal information, and misuse of such information. Many studies has summarized that factors like the perceived possible "Privacy" risk associated with personal information is exposing, and the perceived loss of control over the provided personal information has created such scepticism in the minds of consumers against

154 Hong, W., & Thong, J. Y. L. (2013). Internet "Privacy" concerns: An integrated conceptualization and four empirical studies. MIS Quarterly, 37(1), 275–298

155 CIGI & Ipsos (2018). 2018 CIGI-ipsos global survey on internet security and trust.

service providers[156]. Perceptions of "Privacy" control and hazards not only raise users' "Privacy" worries, but also have the ability to create a climate in which users distrust organisations and are hesitant to give personal information. As a result, organisations must be capable of establishing trust and encouraging people to give personal information. To do so, organisations must first understand how users perceive the "Privacy" assurance mechanisms offered and how these mechanisms are linked to factors influencing users' decisions to disclose personal information, such as perceptions of "Privacy" control and risks, "Privacy" concerns, trusting belief, and behaviour related to personal information disclosure[157].As a result, organisations would benefit from a thorough understanding of how organisational "Privacy" promises relate to users' "Privacy" concerns, perceptions, trust, and information disclosure behaviour to build successful "Privacy" practises and management strategies. The Service providers must ensure the data safety of the consumers and in case of any kind of breach, they should be strictly held liable. In the Digital "Data Protection" Act 2023, the Government of India has taken strong foothold by making sui generis "Data Protection" Norms for the Data fiduciaries.

Importance of Data:

The importance of Data in today's world immeasurable. From the staring our day to it's very ending we either generate a ton of data or consume a ton of Data. In this part of the thesis we are going to understand the importance of data and also discuss about the methods of protecting our data. On the later part, we will also discuss about the liabilities that a service provider carries on their shoulder for protecting our data.

156 Ibid.

157 H., Teo, H., Tan, B. C. Y., & Agarwal, R. (2012). Effects of individual self-protection, industry self-regulation, and government regulation on "Privacy" concerns: A study of location-based services. Information Systems Research, 23(4), 1342–1363. https://doi.org/10.1287/isre.1120.0416

1. **Informed Decision Making:** Businesses, governments, and other organizations can use the insightful information provided by data to make well-informed decisions. Stakeholders can better understand consumer behavior, market dynamics, and operational efficiency by using data analysis to find trends, patterns, and correlations.

2. **Competitive Advantage**: The capacity to efficiently gather, evaluate, and use data can give an important competitive advantage in a variety of industries. Businesses that use data to its fullest potential can outperform their rivals in terms of process optimization, focused marketing campaigns, and faster innovation..

3. **Personalization and Customer Experience**: Businesses can use data to tailor their goods and services to each customer's unique requirements and preferences. Businesses can increase customer satisfaction and loyalty by providing personalized recommendations, offers, and experiences through the analysis of customer data.

4. **Predictive Analytics**: Organizations can use historical data and advanced analytics techniques to forecast future trends and outcomes. Many industries, including marketing, finance, and healthcare, can use predictive analytics to foresee consumer behavior, spot possible hazards, and allocate resources as efficiently as possible.

5. **Research and Development**: Data serves as a foundation for research and development in fields such as healthcare, science, and technology. Researchers can analyze large datasets to gain insights into complex phenomena, discover new patterns, and develop innovative solutions to pressing challenges.

6. **Public Policy and Governance**: Research and development in domains like science, technology, and healthcare are all based on data. Large datasets can be analyzed by researchers to shed light on intricate phenomena, identify fresh patterns, and create ground-breaking answers to urgent problems.

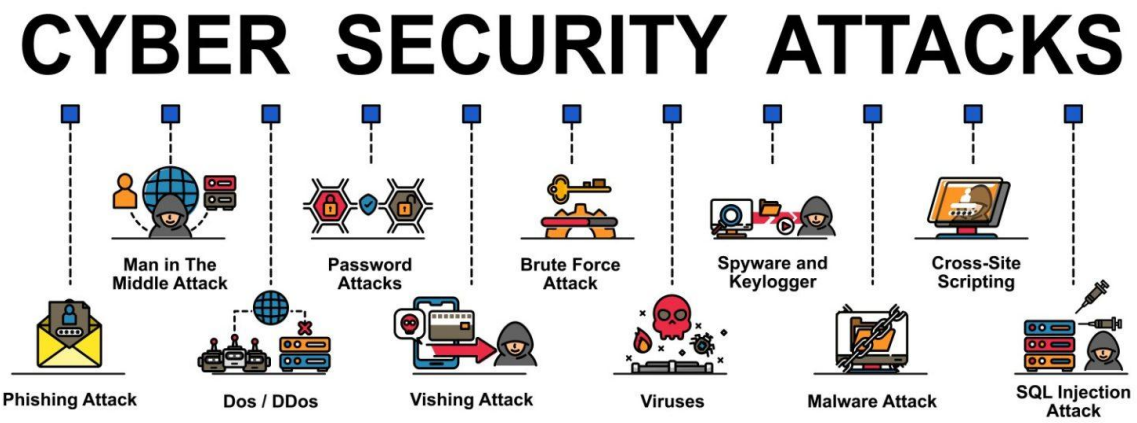
7. **Economic Growth and Innovation**: Globally, data-driven technologies and business models have proliferated, spurring innovation and economic growth. Advances in digital infrastructure and data analytics have led to the rapid expansion of industries like telecommunications, fintech, and e-commerce.

8. **Healthcare and Public Health**: Data is essential to the healthcare industry because it helps with disease surveillance, patient outcomes, and medical research. Healthcare providers can offer individualized treatment and create new therapies with the use of genomic data, medical imaging, and electronic health records.

9. **Protecting Democracy:** In India many Political parties to strengthen their party funds had introduced Electoral Bond System. The best part of the system was no one can demand to know about the amount of such bonds from the donor or the receiver. The Indian Supreme Court has taken the stand that such policy cannot be brought under

the right to “Privacy” or secrecy. The apex Court has taken such decision with the motive to protect the sanctity of fair election and to protect democracy.

Types of Cyber Attack:



158

Cyber attack is unique kind of digital attack where an individual or an association targets another individual or institution with the intention to get a hold on their personal or sensitive information and hold that data hostages for ransom. Now, let us see what methods are usually employed by such criminals:

Phishing:

Phishing is a social engineering technique whereby phony emails or messages are sent to people or organizations in an attempt to trick them into disclosing personal information like passwords and usernames. Phishing attacks are among the most common types of “Cyber Attacks” and are frequently used to obtain access to networks or steal confidential information.

[158] Okan YILDIZ, *The Most Common Methods Used by Cyber Attackers*, SECURE DEBUG (Mar. 31, 2023), https://securedebug.com/the-most-common-methods-used-by-cyber-attackers/ (last visited Feb 15, 2024).

Malware:

Software that is intended to damage a computer system is known as malware. Cybercriminals employ a variety of malicious software, including Trojan horses, worms, and viruses, to infiltrate systems and steal information from computers. Malware can be distributed via social engineering strategies, compromised websites, and email attachments. A fun fact about this malware: most of them are designed by the companies who are selling the anti-dotes or anti viruses.

DOS Attack Method:

Attacks known as denial of service (DoS) aim to overload a system or network with traffic so that users are unable to access it. Botnets, which are networks of compromised computers that cybercriminals can control remotely, are frequently used in denial-of-service attacks. Businesses and organizations, especially those that depend on their online presence for revenue or customer engagement, may experience severe disruptions as a result of these attacks.

Targeting Victim's Password:

To access networks or systems, password attacks use software tools to guess or crack passwords. Password attacks are carried out by cyber attackers using a variety of strategies, including social engineering, dictionary attacks, and brute force attacks. Users with weak or simple-to-guess passwords are prime targets for password attacks.

Man-in-the-Middle (MitM) Attacks:

Intercepting communications between two parties, like a user and a website or application, is known as a man-in-the-middle (MitM) attack. MitM attacks are a useful tool for cybercriminals to introduce malicious code into communications or steal confidential data,

like usernames and passwords. MitM attacks can be executed through a number of techniques, including malware infection of a user's device or WiFi eavesdropping.

SQL Injection:

This type of attack entails inserting malicious code into the SQL database of a website to allow unauthorized users to access confidential information or to manipulate the content of the website.

Case of "Data Breach" and its effect on the Globe:

"Data Breach"es can have an immediate impact on hundreds of millions or even Actions of people in today's data-driven world. The increasing volume of data generated by digital transformation has led to a rise in "Data Breach"es as hackers take advantage of people's reliance on data for everyday tasks. The magnitude of cyberattacks in the future remains uncertain, but this compilation of the worst "Data Breach"es of the 21st century shows that they have already reached massive proportions. The history of "Data Breach"es is evidence of how cyber security is changing and how much of an impact it has on today's world. Every event, from the first instances of illegal access to the large-scale breaches impacting millions of people, has had a profound effect on people, institutions, and society as a whole. This discussion highlights the significance and lessons learned from five key moments in the history of "Data Breach"es.

1. **"Data Breach" at TJX Companies (2007)[159]:**

TJX is a large multinational clothing and home goods retailer operating several brands of stores in the United States, Canada, and Europe. According to Cereola and Cereola (2011), TJX made a significant investment in its information systems and used these IT elements to

[159] Edwin Covert, *Case Study: TJ Maxx's "Data Breach"*, MEDIUM (Oct. 3, 2021), https://medium.com/@edwincovert/case-study-tjx-data-breach-4ace4cc2732a (last visited Feb 15, 2024).

operate its business effectively and efficiently. However, in 2007, TJX disclosed to the public it was the victim of a "Data Breach". Criminals stole over 45 million credit and debit cards, making it one of the largest "Data Breach"es at the time. Following an examination, TJX discovered that threat actors had been present in its IT systems for almost 18 months, from July 2005 to December 2006. In the winter of 2006, TJX notified federal law enforcement and financial regulators about the "Data Breach". In the end, the US Federal Trade Commission (FTC) filed a complaint against TJX, claiming that the company transmitted and stored personal data in clear text, putting unnecessary risks on customer data, didn't have any security measures in place to restrict wireless access to its network, didn't use those that did exist to restrict access between computers and the Internet, and didn't take appropriate steps to detect and prevent unauthorized access. The FTC ordered TJX to appoint a cyber security officer, identify "specific administrative, technical, and physical safeguards and certify their new cybersecurity program was operating efficiently each year for the next twenty years. In addition, TJX paid nearly $41 million to VISA, $24 million to MasterCard, and attorneys general of multiple states to prove their IT systems were secure and pay restitution to affected customers for direct harm and for credit monitoring. The total cost of the "Data Breach" to TJX exceeded $250 million.

2. **Yahoo "Data Breach"**[160]:

Yahoo, a well-known provider of internet services, suffered two massive "Data Breach"es in 2013 and 2014 that were previously unheard of in scope. These breaches resulted in the theft and unauthorized access of private data belonging to Actions of Yahoo users. Due to the seriousness of these breaches, a vast amount of personal data was compromised, making it

[160] Shellmates Club, *Yahoo "Data Breach": An In-Depth Analysis of One of the Most Significant "Data Breach"es in History*, MEDIUM (Jul. 23, 2023), https://shellmates.medium.com/yahoo-data-breach-an-in-depth-analysis-of-one-of-the-most-significant-data-breaches-in-history-ba5b46be560b (last visited Feb 15, 2024).

one of the biggest "Data Breach"es in history. When Yahoo first experienced a breach in 2013, a whopping 3 Action accounts were compromised, along with a wealth of private data. Phone numbers, encrypted passwords, email addresses, birth dates, and usernames were among the compromised data. Yahoo's enormous user base was greatly impacted by this widespread infiltration, raising serious concerns about the possible misuse of the stolen data. After that, Yahoo experienced yet another serious "Data Breach" in 2014 that compromised the accounts of about 500 million users. Unauthorized actors were able to access a plethora of personal data, including encrypted passwords, phone numbers, email addresses, and birth dates, as a result of this breach. The magnitude and breadth of this breach further compounded the vulnerabilities that Yahoo's user community was already facing, raising concerns about cyber security and data "Privacy".

3. **Equifax "Data Breach"**[161]:

The Equifax company was founded in the late 19th century as retail credit company. With the advent of time it created a multi Action dollar industry by gathering financial and personal data of almost all the Americans. They mainly ran their business by analysing the financial condition of their clients and selling them to the bank or lenders. They were so successful in their business that they had to open many service centres all over USA. 'It is said that the biggest tree in the jungle falls the quickest'. Same happended with Equifax. They were so busy in minting money that, they kept hidden doors open for the online Thieves. Hackers from all over the world entered their servers freely and stole away data worth of "143 million" users. Equifax was so unprepared for this cyber attack on them that just to close and clear their server at Atlanta it took them 11 days. With the Federal Trade Commission, the Consumer Financial Protection Bureau, and all "50 states and territories of the United States"

[161] Equifax "Data Breach" FAQ: What happened, who was affected, what was the impact?, CSO ONLINE, https://www.csoonline.com/article/567833/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html (last visited Feb 15, 2024).

the company has consented to a global settlement. Up to $425 million in compensation is part of the settlement to assist those impacted by the "Data Breach".

4. **Cambridge Analytica Scandal**[162]:

Numerous respondents filled out a similar survey in 2014, which combined the user's personally identifiable information with Facebook friends' data from the business that backed President Trump's 2016 campaign. At this point, Cambridge Analytica (CA) and UK researcher Aleksandr Kogan entered the picture. Kogan was using Facebook for research. Kogan sent a survey to 3L Americans that appeared innocuous and included over 100 personality traits with which respondents could agree or disagree. However, there is a catch: to complete the survey, respondents must sign up or log in to Facebook, which gives Kogan access to the user's location, birthdate, and profile. By merging the survey data with the user's Facebook information, Kogan produced a psychometric model that resembles a personality profile. Kogan then merged the data with voter records and forwarded it to CA. According to CA, the survey results were essential in figuring out how they profiled a user's psychoneurosis and other susceptible traits, along with the individual characteristics of different users and models. Two lakh twenty thousand people participated in Kogan's survey in a matter of months, and information from as many as 87 million Facebook user profiles nearly a quarter of all Facebook users in the US was obtained. Although the campaign objected, the plan was to use the data to target users and/or survey respondents with political messaging that would support Trump's campaign strategy. Kogan shared the developed data with CA despite the fact that his work was for academic research, which is against Facebook policy.

[162] Julia Carrie Wong, *The Cambridge Analytica Scandal Changed the World – but It Didn't Change Facebook*, THE GUARDIAN, Mar. 18, 2019, https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook (last visited Feb 15, 2024).

5. **Adhar "Data Breach"**[163]:

Early in 2018, reports surfaced that malevolent actors had gained access to Aadhaar, the largest ID database in the world, revealing personal information on over 1.1 Action Indian citizens, including names, addresses, phone numbers, emails, and biometric information like fingerprint and iris scans. Furthermore, it was a credit breach as well because the database, created by the Unique Identification Authority of India (UIDAI) in 2009, contained data on bank accounts linked to distinct 12-digit numbers. This was true even though the UIDAI first denied that the information was in the database. Via the website of Indane, a state-owned utility company connected to the government database via an "application programming interface" (API) that let apps retrieve data stored by other apps or software, the actors gained access to the Aadhaar database. Sadly, Indane's API lacked access controls, making its information vulnerable. Through a WhatsApp group, hackers offered access to the data for as little as $7. The vulnerable access point was not taken offline by Indian authorities until March 23, 2018, despite warnings from tech groups and security researchers. However, if you search about this breach on the internet now it will in bold letters will show you that 'Never been breached'.

6. **Solar Winds Supply Chain Attack:**

[163] Aadhaar details of 81.5 cr people leaked in India's 'biggest' "Data Breach", HINDUSTAN TIMES (2023), https://www.hindustantimes.com/technology/in-indias-biggest-data-breach-personal-information-of-81-5-crore-people-leaked-101698719306335.html (last visited Feb 15, 2024).

Based in Tulsa, Oklahoma, SolarWinds was a well-known software provider that offered technical services and system management tools for network and infrastructure monitoring to hundreds of thousands of businesses worldwide. One of the company's offerings is the Orion IT performance monitoring system. Solar Winds Orion has special access to IT systems as an IT monitoring system, allowing it to collect log and system performance data. Because of its advantageous position and extensive deployment, Solar Winds was a desirable and profitable target. Thousands of Solar Winds customers' networks, systems, and data were made accessible to a group known as Solar Winds. The hack's scope is unparalleled and among the biggest—if not the biggest—of its kind that has ever been documented. The Orion network management system is used by over 30,000 public and private organizations, including local, state, and federal agencies, to manage their IT resources. As a result, when SolarWinds unintentionally distributed the backdoor malware as an update to the Orion software, the hack compromised thousands of people's data, networks, and systems. Not just customers of Solar Winds were impacted. As a result of the hack exposing the internal operations of Orion users, the hackers may also be able to access the information and networks of their partners and clients, which would allow the number of impacted victims to increase dramatically. The malicious code that the hackers inserted into the Orion system was done so through a technique called a supply chain attack. A supply chain attack operates differently from a network hacking attack in that it goes after a third party that has access to an organization's systems. Hackers can impersonate users and accounts of victim organizations by creating a backdoor through third-party software, in this case the Solar Winds Orion Platform. Even antivirus software might miss the malware's ability to access system files and blend in with genuine Solar Winds activity. From the initial day of the first attack it took ninety plus days for security agencies to find out about the attack.

7. LinkedIn "Data Breach"[164]:

In June 2021 LinkedIn discovered that 700 million of its users' data had been posted on a dark web forum, affecting over 90% of its user base. By abusing the site's (and others') API, a hacker going by the handle "God User" employed data scraping techniques to dump a first information data set that included roughly 500 million customers. They boasted that they were selling the entire 700 million customer database after that. LinkedIn contended that the incident was a breach of its terms of service rather than a "Data Breach" because no private, sensitive information was disclosed; however, a data sample that was scraped and posted by a God User included information such as phone numbers, email addresses, genders, and other social media details, which would provide malicious actors with plenty of information to craft plausible, subsequent social engineering attacks following the leak, as cautioned by the UK's NCSC.

8. Marriott International:

After an attack on its systems in September 2018, "Hotel Marriot International" revealed that private information belonging to half a million Starwood guests had been made public. The massive hotel chain released the following statement in November of that year: On September 8, 2018, Marriott received a notice from an internal security tool about an attempt to gain access to the Starwood guest reservation database. Marriott contacted top security specialists right away to assist in figuring out what had

[164] Brandon Gibson et al., *Vulnerability in Massive API Scraping: 2021 LinkedIn "Data Breach", in* 2021 INTERNATIONAL CONFERENCE ON COMPUTATIONAL SCIENCE AND COMPUTATIONAL INTELLIGENCE (CSCI) 777 (2021), https://ieeexplore.ieee.org/document/9799221 (last visited Feb 15, 2024).

happened. During the course of the investigation, Marriott discovered that there had been unlawful access to the Starwood network since 2014. Following its discovery, Marriott moved to have the information that had been encrypted and copied by an unauthorized party removed. The statement also stated that Marriott was able to decrypt the data on November 19, 2018, and discovered that the contents came from the Starwood guest reservation database. The names, postal addresses, phone numbers, email addresses, passport numbers, Starwood Preferred Guest account information, dates of birth, gender, arrival and departure details, reservation dates, and communication preferences of the guests were among the information that was copied. Payment card numbers and expiration dates were also included for some of the records, though they were reportedly encrypted. The names, postal addresses, phone numbers, email addresses, passport numbers, Starwood Preferred Guest account information, dates of birth, gender, arrival and departure details, reservation dates, and communication preferences of the guests were among the information that was copied. Payment card numbers and expiration dates were also included for some of the records, though they were reportedly encrypted. Following the breach, Marriot announced plans to phase out Starwood systems and expedite security enhancements to its network. The company also conducted an investigation with the assistance of security experts. The Information Commissioner's Office (ICO), a UK data regulatory body, ultimately fined the company £18.4 million (down from £99 million) in 2020 for failing to protect the "Privacy" of its customers' personal information.

Effects of Data and "Privacy" Loss: A study on global Scale.

World has suffered from enough losses due to "Data Breach", however it is difficult to provide any exact figure about such loss. In this part of our discussion we will discuss about the types of damages that a country suffers due to breach of "Privacy" and Data Loss.

Direct and Indirect Loss:

There are "two types" of financial losses that can arise from a "Data Breach": direct and indirect. Paying fines, settling potential lawsuits, and hardening systems are examples of direct costs. Reductions in revenue as a result of a tarnished reputation, the loss of current clients, etc. are examples of indirect costs. The actual consequences of the compromised data, which may reveal proprietary tool information, company IT secrets, and more, are not included in this monetary loss. All of this has a significant impact on how the public views your business and how confidently customers believe you can safeguard their private information. One such instance is the well-known 2014 Sony "Data Breach", which was estimated to have cost $35 million. This amount accounts for both visible and hidden costs of financial loss, such as hardening the infrastructure through the hiring of contractors and forensics experts, conducting investigations, paying fines, and dealing with lawsuits. These hidden costs include a drop in business revenue as a result of a drop in customer purchases, which is connected to a decline in the customers' favourable perception of the company. The bottom line of your company may be strongly impacted by both expenses.

Productivity Losses:

Money is just the tip of the iceberg in terms of data loss. One unintended consequence of data loss is lost productivity, which can be very costly for companies. This can happen when workers are forced to work offline due to sluggish or unresponsive networks. Moreover, staff searching for misplaced data can significantly lower output. Companies still have to pay for network, storage, and employee salaries even when their IT infrastructure is idle.

Intellectual Property Theft:

The sphere of Intellectual property is huge. It takes years of perseverance, countless hours of experiments, designs to create an Idea, Expression or innovation. It will not be wrong to say that sometimes IPR becomes identity for a person. Imagine how will you feel if your identity is stolen. One might ask, what comes under the purview of IPR? IPR includes Rights related to Copy Right, Patent, and Trade Secrets etc. It is well known fact that it takes lots of revenue, efforts, and time to develop such Intellectual property. If such properties are stolen or violated it will not only put the R&D in behind, it will also put companies behind time. In today's comparative world every single second counts, and if any institution falls behind a year or looses it customer faith, it will not only impact their revenue, it will have a direct impact over millions of jobs and on a greater stage it will directly impact that country's economy. In the initial stage of this article we have discussed about the various instance when Global companies has sustained damages in terms of customer base, now if we change 1 dollar against 1 customer we will see that, the total worth of damage will be in Actions of dollars.

Understanding the Concept of Strict Liability:

Strict liability is the legal concept that holds a defendant accountable for their actions regardless of their intent or mental state at the time of the action, both in criminal and tort law. Strict liability offenses in criminal law include, for example, statutory rape and possession crimes. Strict liability in criminal law usually applies only to minor offenses. Strict liability is one of five mens reae (mental states) that a defendant may experience while pursuing a crime, according to criminal law. "Acting with recklessness," "behaving with negligence," "acting purposefully," and "knowing" are the other four. Penalties for the mens rea of strict liability are generally less severe than those for the other four mentes reae. One may say that, Strict liability is a concept in Tort, why are you mixing this in Right to

"Privacy".to answer this, I would like to point out to the discussion that in most of the cases of "Data Breach", the data fiduciaries were either not aware about the breach in their system or were negligent when securing their data repositories from any kind of unwanted intrusion. The case study of Cambriedge analytica shows that, the whole incident actually started from an educational servey and ended into the biggest data scam of twenty first century. Similarly other "Data Breach"es like Norton, Facebook, Marriot were either results of faulty security system or due to lack of proper ombudsmen. It is necessary to mention here that, although big companies lost their data but we lost our identity. No one can guarantee us that our data will not be used for any unlawful activities or for any other activities which we will normally avoid. In any of such adverse scenarios if our digital identities are used for any unlawfull activities it will be very difficult to prove our innocence before the law enforcing authorities.

Now, the question remains, who shall be guilty for such unprecedented incident? The original culprits who has carried out the "Data Breach" or the data fiduciaries who has knowingly or unknowingly has left their door open for the thieves who were sniffing for a chance to steal our data. The concept of Strict Liability states that, in a given condition when a party suffer losses due to the negligence of another party, then in such a scenario the party who was negligent should be held guilty. In the world of "Data Breach" the data fiduciaries has the responsibility to properly protect our data which we entrusted to them. In case such breach happens due to their fault, they should be strictly liable towards the victim. In developed economy such USA, UK they have dedicated legislations for this purpose. In India we have recently updated our legislation related to "Data Protection" and in the new regime we have enacted strategies to handle such kind of "Data Breach" and have also dealt with the fixing liability in such kind of "Data Breach".

Protecting Data from Potential threats:

It is said that Prevention is always better than cure. Similarly in data industry it is always better to pay close attention towards Protection mechanism as early as possible rather than paying compensation to

the victims. The best way out is sensitization among the data fiduciaries and the customers. In this part of the chapter, we are going to discuss various ways through which Data can be protected.

1. **Educating employees on the dangers of "Cyber Attacks":**

According to an IBM "Data Breach" report[165], the average cost of a security breach in the US was predicted to reach $9.05 million in 2022; a significant factor in this estimate was the increase in remote work. Furthermore, phishing emails are the initial stage of about 91% of "Cyber Attacks", and they are also linked to 90% of "Data Breach"es. Fortunately, effective cybersecurity training and a focus on upholding a company's security compliance can frequently prevent this kind of harm. Humans are a major cyber risk, but that risk can be decreased by putting certain strategies into place like cybersecurity awareness training. Employees with cybersecurity training are no longer viewed as the "weakest link" in the security measures of the organization. Employees with training are better equipped to recognize and react to "Cyber Attacks" such as malware and phishing. Cybersecurity education can be provided in a number of ways, such as through the use of simulated breaches, risk analysis, software, video, or demonstrations in a classroom setting. Employees ought to be able to use the Internet safely and wisely after obtaining the necessary training. Any business must prioritize security, and cybersecurity awareness training helps to do just that. Chief information security officers (CISOs) must first increase cybersecurity awareness within their organizations to establish a cybersecurity culture. The best way to establish a cyber security culture is to start at the top and work your way down. Leaders who prioritize cybersecurity will inspire the rest of the staff to follow suit. Employee adherence to cybersecurity protocols will be automatic in such a culture, negating the need for ongoing training. A company's reputation is safeguarded and potential fines are avoided when

[165] Cost of a "Data Breach" Report 2023.

compliance management is given top priority as part of the cybersecurity plan. Employee training is emphasized by numerous regulations, such as the CCPA, GDPR, PCI-DSS, and HIPAA. Mandatory compliance requirements in many sectors are satisfied by incorporating pertinent training materials.

2. **Implementing strong password policies and multi-factor authentication:**

Your systems and network don't always need to be protected by a strict password policy. Multi-factor authentication adds more security layers to safeguard users and resources. You can require users to authenticate themselves using a different password, a different device, or a piece of biometric data by implementing two-factor authentication. Because of this, user accounts can be safeguarded by this extra security layer, even in the event that a hacker manages to get the right username and password. An effective password policy can make a big difference in how secure the data of your users is. Your website should provide clear instructions on how to create secure passwords for users who are not familiar with the process. This can assist in keeping them from doing things that could jeopardize their data and leave them vulnerable to dangers. Data fiduciaries can significantly lower the risk of security breaches, safeguard sensitive user data, and guarantee transparency by putting in place a strong password policy and offering guidance to users.

3. **Keeping software and systems up-to-date with the latest security patches:**

Patches for vulnerabilities or bugs that hackers might use to access your system or data are frequently included in software updates. Installing the most recent updates can lower your risk of “Cyber Attacks” and safeguard your company's and personal data. The main justification for updating software right away is security. Vulnerabilities in software allow hackers to gain access to an individual's computer. Threat actors view these weaknesses as

openings that let them infect computers with malware. Threat actors can take over computers and steal data thanks to malware. To render files, documents, and other programs useless, malware can also encrypt them. Security patches close these software gaps, shielding a device from intrusions. Individuals who share a network with others must exercise extra caution. Unknowingly, an infected device can transfer malware to friends, family, coworkers, and other network users. A threat actor will look for sensitive documents, usernames, passwords, financial information, and other personal data if they gain access through a software security loop. Threat actors gain access to private accounts and resell confidential data on the dark web. Data can be better protected by updating software to address security flaws. For instance, a stolen VPN password led to the 2021 Colonial Pipeline hack.

4. **Using anti-virus and anti-malware software to protect against malicious software:**

Malware, including viruses, Trojan horses, ransomware, and rootkits, is one of the most prevalent and frequent cyber threats businesses encounter. In fact, the number of malware attacks worldwide in 2022 was an astounding 5.5 Action. Furthermore, in 2022, ransom ware a particular type of malware cost businesses $4.54 million on average. Because hackers and other bad actors use a wide range of malware, anti-malware software is critical to an organization's overall cyber security posture. Even worse, cybercriminals are always creating new kinds of malware, and each iteration gets more advanced and lethal than the last. Look no further than Ransom ware-as-a-Service (RaaS), an increasingly convenient way for aspiring cybercriminals to obtain the malware they need. Apart from these, mal wares are used for stealing private information, erasing, changing, or destroying data exhilaration or encryption to make money (ransom ware), gaining access to digital assets and third-party software that are available to an organization; connecting to devices and taking control

remotely at any time; and stealing user sessions, i.e., pretending to be an employee and navigating in any network with their access rights, recording user behavior, such as entering their login credentials affecting the performance of the device and the network, sending users to malicious websites of their choosing after rerouting them from their requested addresses, completely prohibiting users from using the internet, and displaying unsolicited pop-up ads regularly. All of these can be avoided just by updating anti virus.

5. **Monitoring network traffic for suspicious activity and implementing firewalls and intrusion detection systems:**

A technological tool called an intrusion detection system (IDS)[166] keeps an eye on all incoming and outgoing network traffic to look for unusual activity or policy violations. An intrusion detection system's main goal is to identify and stop intrusions into your IT infrastructure, as its name implies, and then notify the appropriate parties. These remedies may take the form of software programs or hardware products. An information and event management system of greater size will usually include an intrusion detection system (IDS). Your IDS serves as your first line of defense when it is integrated into a comprehensive system. It reduces the mean time to detect and proactively identify anomalous behaviour. In the end, the sooner an attempt or intrusion is discovered, the faster you can take appropriate action and make the system safe for intended users.

6. **Conducting regular security audits to identify vulnerabilities and address them before they can be exploited by cyber attackers:**

The likelihood of "Cyber Attacks" increases as the world grows more interconnected. An effective cyber security management system must be in place to protect against these threats.

[166] Human Marketing, *Understanding the 5 Types of Intrusion Detection Systems*, HELIXSTORM (Aug. 18, 2022), https://www.helixstorm.com/blog/types-of-intrusion-detection-systems/ (last visited Feb 17, 2024).

Regularly carrying out comprehensive cyber security audits is an essential component of this procedure. Your IT infrastructure is thoroughly analyzed and reviewed as part of a cybersecurity audit. It identifies risks and vulnerabilities, highlighting high-risk behaviors and weak points. Enhanced security measures, risk assessment and vulnerability identification, and compliance with rules and standards are some of the major advantages of IT security audits, being ready for emergencies, protecting private information and customer confidence, and proactively identifying and thwarting threats.

Sollutions to Data Breach and Importance of E- Prior Informed Contracts:

Are you a Robot? This is the most frequently asked question over the Internet. Let me tell you what is going to be the next frequently asked question over the Internet in the next decade. It will be- Are you an AI?

One might think, the websites are just securing their data base from any kind of unwanted AI interference or may be protecting their system from "Data Breach". This may be the case, however most of the time they just wants to follow the behavioral pattern of a customer in their website, so that they can lure them with consumer products of his/her liking. Furthermore, whenever we are browsing over the Internet, and a question pops out, "Do you agree to the terms and Condition of using this website or the terms of the service, we simply click on the disastrous button of "AGREED". Well, it will be completely wrong to blame the service providers, we as consumers have also the duty to be vigilant and do justice to the word "caveat emptor". Although most of us choose to ignore this due to the long list of terms and condition. Although we may assume that lengthy terms and conditions are standard, is there any way they may be condensed and made more user-friendly for all of us?

The advent of Big Data and fusion centers, data security breaches, the rise of Web 2.0, rising marketing, and the expansion of monitoring technology have all exacerbated “Privacy” issues during the last decade. Policymakers in developed and developing countries have proposed and passed substantial new regulations, but the underlying approach to preserving “Privacy” has remained largely intact since the 1970s. The law currently offers people some rights that allow them to decide how to manage their data. These rights essentially include the rights to be notified, to access, and to consent to the collection, use, and disclosure of personal data. The purpose of this set of rights is to provide people control over their personal data, so that they can balance the costs and benefits of the acquisition, use, or disclosure of their information for themselves. In this era of e-consent management of “Privacy” is very important. Let us discuss what issues one individual may face during managing their consent and managing their “Privacy”.

How Prior Informed Contract Works:

A contract is the outcome of a negotiation process between parties who exercise their freedom to contract, according to the fundamental paradigm of contract law. On the other hand, Ss are rarely the result of any negotiation and are instead provided on a take-it-or-leave-it basis. SFECs contain clauses that are decided upon beforehand by one party and are better in terms of market dominance and negotiating. Usually, the only people who negotiate and enter into contracts with individual customers are the seller's agents. Typically, these agents aren't allowed to alter or compromise the standard agreements they provide.

Standard form contracts (also known as "SFECs")[167] have been used for many years to facilitate and carry out a wide range of consumer transactions between businesses and individuals. Form contracting will probably remain the most common approach as new and

[167] W. David Slawson, *Standard Form Contracts and Democratic Control of Lawmaking Power*, 84 HARVARD LAW REVIEW 529 (1971).

improved standard contracting practices are introduced into the market by contemporary technology and developments. One well-known example is online contracting, which is continuously expanding both in size and scope. Standard terms included in SFECs regulate almost all online interactions. Within this larger feature, retail transactions—also known as business-to-consumer transactions are dominated by online standard contracting[168]. If we take reference from Indian contract act, precisely the definition itself suggests that an agreement enforceable by law[169] becomes a contract[170]. If we analyse this definition, we find that there must be some kind of consideration in terms of monetary or services to enforce any kind of contract. However, in standard form of e-contracts the service providers in exchange for giving us the right to use their platform wants us to share the right to "Privacy" with them.

If I am not wrong, "Privacy" can't be shared with anyone. In-todays term if you want to use the platform of private banking app (For example ICICI, HDPC- for credit card usage) they may require you to give up your DNC rights. Now, one might ask, what are our DNC Rights?

DNC Rights are those right who protect us from any kind of unwanted instrusion from on-line service providers to protect our "Privacy". Let us a have a quick look, at the DNC Right:

1. Telemarketers Customers or e-service providers can only be contacted by telemarketers during specific hours.
2. It is forbidden for telemarketers or e-service providers to use dishonest tactics.
3. It is forbidden for telemarketers or e-service providers to get in touch with customers listed on the DNC registry.

[168] Jason Scott Johnston, *The Return of Bargain: An Economic Theory of How Standard Form Contracts Enable Cooperative Negotiation between Businesses and Consumers*, SSRN JOURNAL (2006), http://www.ssrn.com/abstract=881074 (last visited Feb 10, 2024).
[169] Section 2(h) of the Indian contract act. 1872.
[170] India Code: Section Details, https://www.indiacode.nic.in/show-data?actid=AC_CEN_3_20_00035_187209_1523268996428&sectionId=38605&sectionno=2&orderno=2 (last visited Feb 10, 2024).

4. It is mandatory for telemarketers or e-service providers to remove any registered number from their call lists and to search the registry at least once every thirty-one days.
5. Businesses need to keep an internal DNC list up to date. have to identify themselves and the companies they work with.
6. Requests to have a phone number added to an internal DNC list ought to be complied with right away and kept there until the customer decides to re-opt in.
7. If any business choose to violate these right they will be fined financially.

Now, if we are required to give-up these rights and the businesses tricks us to give up these rights our "Privacy" will be bombarded with unwanted intrusion by way of continues calls, spam emails and what not. The main scope of a contract is to benefit both the parties, not just one party at the cost of another's damage.

It is pertinent to mention here that in Standard form of e-contract, has only one kind of consideration involved, that is ***You let me violate your "Privacy" and in-ex-change I will let you use my platform, while you leave back some digital foot-print and I can track you back with it.*** Additionally, while businesses have countless opportunities to draft and litigate contracts, they are sophisticated "repeat players," whereas consumers are typically "one-shot players[171]." These factors may make the difference in the bargaining power between businesses and individual customers greater.

Standard Form of E-Contracts vs Legalonomy (Legal Economy):

The distinct characteristics of SFECs, as previously mentioned, have almost made them disparaging. Courts, lawmakers, scholars, and the general public all frequently criticize

[171] Marc Galanter, *Why the "Haves" Come Out Ahead: Speculations on the Limits of Legal Change*, *in* DISCUSSIONS IN DISPUTE RESOLUTION: THE FOUNDATIONAL ARTICLES 0 (Art Hinshaw, Andrea Kupfer Schneider, & Sarah Rudolph Cole eds., 2021), https://doi.org/10.1093/oso/9780197513248.003.0061 (last visited Feb 10, 2024).

standard form e-contracts. However, when looking at SFECs from a traditional legal and economics standpoint, the majority of the traditional accusations—such as the offer of form contracts by agents who are not authorized to make contextual changes, execution between unfamiliar parties, and inequality in economic strength—do not always present a serious threat to contract law. The fundamental ideas of law and economics, or L&E for short, hold that both parties to a contract will only agree to terms that are efficient and maximize their respective benefits.[172] Furthermore, there are numerous benefits to businesses using SFeCs generally. By doing away with the need for contractual term negotiations, the SFeCs significantly lower transaction costs. Through SFECs, vendors can also save money by paying less for the training of their agents and staff. By acting as a repeated check on selling agents who might be too eager to make offers that conflict with the vendor's interests, the SFeC helps to increase the efficiency of the vendor as well. Given that every customer receives the same contract, SFeCs can represent equality among customers (provided that the vendor refrains from discriminatory contract terms), boosting customers' trust. Finally, it is believed that open market transactions involving SFeCs advance the interests of both parties. Consumer SFeCs are essentially non-negotiable, but it is expected that both businesses and consumers will profit from these agreements[173]. Consequently, rather than focusing on the nuances of the SFeCs, contract law should only aim to address market failures that impair the parties' ability to maximize their utility. The ability of courts to determine what, ex post, would have been a reasonable contractual distribution of risks and obligations among the parties ex-ante is questioned by commentators. Most of the time, courts lack the knowledge required to evaluate the particular market and transaction that a given SFeC[174] deals with. Courts may also find it challenging to comprehend the relationship between benefits provided

[172] Clayton P Gillette, *PRE-APPROVED CONTRACTS FOR INTERNET COMMERCE*, HOUSTON LAW REVIEW.
[173] *Id.*
[174] R Ted Cruz & Jeffrey J Hinck, *Not My Brother's Keeper: The Inability of an Informed Minority to Correct for Imperfect Information*, 47 HASTINGS LAW JOURNAL.

by one contractual provision and concessions made in another. Legal interference that infringes on the autonomy of the contracting parties falls under the definition of overt state paternalism under SFeCs. According to some scholars, the fact that companies are repeat customers puts them in the best position to judge what should be included in form contracts[175].

Standard From of E-Contract vs. The Policy Frames: A New Approach.

The foundation of the Non-Intervention Approach, or NIA, is the force of competition in the market. It is said that these forces produce the ideal balance, where vendors are sufficiently motivated to draft effective, standardized terms[176]. The NIA's proponents admit that customers usually don't read the terms of SFECs before completing a transaction. However, in markets where there is competition, the fact that some customers (referred to as Marginal Consumers) read the terms of the contracts and are prepared to look for better terms should be sufficient. This means that a vendor who includes unfair or unjust clauses in their agreement runs the risk of losing Marginal Customers to a rival who provides better terms. In competitive markets, companies are unlikely to take advantage of consumers by enclosing self-serving contract clauses in SFECs, as long as they respond to consumers collectively and offer products that align with their preferences[177]. Because of this, the NIA depends on the existence of market pressure, which is produced by a significant subset of marginal consumers. Only in markets where the costs of extorting infra-marginal consumers—who are still subject to unfair and biased contractual provisions—will outweigh the benefits of losing marginal consumers as a result of unfair contractual terms will such a dynamic materialize.

[175] Robert A Hillman, *Rolling Contracts*, 71 FORDHAM LAW REVIEW.
[176] Alan Schwartz & Louis L. Wilde, *Imperfect Information in Markets for Contract Terms: The Examples of Warranties and Security Interests*, 69 VIRGINIA LAW REVIEW 1387 (1983).
[177] Alan Schwartz, *Unconscionability and Imperfect Information: A Research Agenda*, 19.

The policy response to the concern over unfair SFeCs should be restricted to promoting the use of short, straightforward contracts, keeping the NIA in mind. This will help Marginal Customers express their dissatisfaction with the provided SFeC. Regulators should also support competition because it will give Marginal Consumers more clout and guarantee that they have enough options to choose from, allowing them to express their displeasure with biased SFeCs[178].

Firstly, Many have also questioned the NIA from the perspective of behavioral L&E, a more recent interdisciplinary field. By using this strategy, critics hope to bolster their argument that readers of SFECs are unlikely to read them and are unlikely to comprehend what they contain. In this section, we go over four distinct behavioral patterns that are especially pertinent to standard form contracting procedures.[179] As Russell Korobkin elucidates, consumers tend to concentrate on a limited number of components due to the information overload they encounter when interacting with SFECs. These are usually the clauses in the contract that deal with the price and other obvious (or "salient") features of the product. Non-essential clauses, such as those about forum selection, choice of law, remedies for breaches, exchange policies, etc., are disregarded by customers[180].

Secondly, customers frequently enter SFeCs in an unfavorable environment. Noise, time constraints, and vendor manipulation of customers are often features of the setting and environment where SFeCs are formulated. These elements hinder customers from making a rational, let alone ideal, decision about whether to enter the SFeC[181].

[178] Schwartz and Wilde, *supra* note 10.
[179] Samuel Becher, *Behavioral Science and Consumer Standard Form Contracts*, (2007), https://papers.ssrn.com/abstract=1016002 (last visited Feb 11, 2024).
[180] *Id.*
[181] Sunstein, C. R. (2000). Introduction. In C. R. Sunstein (Ed.), *Behavioral Law and Economics* (pp. 1–10). introduction, Cambridge: Cambridge University Press.

Third, consumers are not always able to assess the likelihood of upcoming risks and contingencies, particularly when those likelihoods involve unpleasant circumstances. Unpleasant occurrences like legal disputes and payment defaults are covered by the majority of SFEC terms. The reason that the majority of SFEC terms are incorrectly evaluated can be attributed to the availability cascade and the predominance of self-serving biases like overconfidence and over optimism[182].

The basis of the fourth behavioral argument is the observation that customers typically visit the SFEC following an extended period of e-commerce. Customers are unlikely to understand the significance or full meaning of the applicable contract at this point. Psychological concepts like cognitive dissonance and the sunk cost effect provide an explanation for this. Because of these occurrences, customers experience a lack of self-commitment, which is also a result of their pre-contractual time and effort commitment[183]. Customers' perceptions of SFECs are skewed, and their willingness to read the contract and take appropriate action is compromised[184].

Both NIA supporters and opponents concentrate on an ex ante analysis, despite having very different perspectives on the dynamics that lead to the formation of SFECs. Both methods look at what customers will do when the contract is being formed. Ex post, when consumers are much more likely to read SFECs or negotiate for changes, is a crucial point that we feel is overlooked by this focus[185]. After the contract is formed, consumers may read and review SFECs with far greater interest and attention than they did before. Examining SFECs in the

[182] Becher, *supra* note 13.
[183] Hal Arkes & Catherine Blumer, *The Psychology of Sunk Cost*, 35 ORGANIZATIONAL BEHAVIOR AND HUMAN DECISION PROCESSES 124 (1985).
[184] Chris Ann Dickerson et al., *Using Cognitive Dissonance to Encourage Water Conservation1*, 22 JOURNAL OF APPLIED SOCIAL PSYCHOLOGY 841 (1992).
[185] Kal Raustiala, *Form and Substance in International Agreements*, 99 AMERICAN JOURNAL OF INTERNATIONAL LAW 581 (2005).

online context requires us to change our attention to this ex post dynamic, as the following Part demonstrates[186].

Right to "Privacy" and analysis of Ex-post and Ex-Ante information Flow:

As previously indicated, consumers in B2C transactions are either unable or unwilling to read SFECs before and during the time of their formation. This might allow vendors to include terms in contracts that are biased[187]. This issue might be lessened by the information that consumers who read SFECs after they publish are releasing to the market. Customers who are informed about biased language may decide not to work with a particular vendor if the results of that contract are ineffective. To prevent losing customers, this information flow would deter vendors from putting unfair and biased clauses in their SFECs in the first place.

The meaning, components, and difficulties with such a data flow are explained in the ensuing paragraphs at three significant "chokepoints":

(1) The ex-post view of the contract;

(2) The information flow from the ex-post to the ex-ante consumer regarding the contract; and

(3) The use and reliance of such information by the ex-ante consumer.

The ex-post view of the contract:

First, we need to figure out why and when customers review SFECs after they have expired. Finding examples of situations where the vendor's actions fall short of the customer's expectations- such as when the product is defective, arrives late or damaged, or fails—is crucial to this interaction (We have to also take in consideration of the return policies applied

[186] Shmuel Becher & Esther Unger-Aviram, *Myth and Reality in Consumer Contracting Behavior*, SSRN ELECTRONIC JOURNAL (2008).
[187] Unconscionability in Standard Forms, CALIF. L. REV. (1976).

by different online market places). In these situations, the customer may feel wronged and look for appropriate redress. Certain disgruntled customers (or their attorneys) may review the SFEC they initially signed with the vendor to familiarize themselves with their rights and responsibilities. Others will complain and seek redress by getting in touch with the relevant vendor. Vendors will then usually refer to the applicable SFEC to inform customers of their rights or lack thereof. Customers may review the SFEC in response and decide what to do next. These and additional behavioral patterns show that customers are highly motivated to look at SFECs after[188].

Customers frequently discover the true nature of their contracts accidentally. In these situations, consumers perceive and comprehend disagreements over “contractual terms and conditions” in an abstract sense, failing to recognize that the true origin of these disputes lies in a standard provision. For instance, in the context of travel, changing the date of a trip can occasionally be costly or challenging after tickets have been purchased. It is unlikely that consumers will fully understand that the problematic SFEC provision divides risks among “the parties to the contract”. However, these dissatisfied customers rail against the carrier for their "lousy customer service," "unfairness," and "lack of flexibility." Consumers do not link the issue to a standard term that they purportedly accepted when purchasing the ticket. However, they specifically criticize certain clauses in the contract[189]. The ex-post context is not affected by the majority of the factors that contribute to ineffective reading and comprehension of "non-salient" terms ex-ante. For example, numerous academics have clarified that, considering the significant burden that reading SFECs would entail, the expenses associated with routinely reviewing them ex-ante will discourage nearly all

[188] Douglas G. Baird, *The Boilerplate Puzzle*, *in* BOILERPLATE 131 (Omri Ben-Shahar ed., 1 ed. 2007), https://www.cambridge.org/core/product/identifier/CBO9780511611179A018/type/book_part (last visited Feb 11, 2024).
[189] Russell Korobkin, *Bounded Rationality, Standard Form Contracts, and Unconscionability*, 70 UNIVERSITY OF CHICAGO LAW REVIEW (2003), https://chicagounbound.uchicago.edu/uclrev/vol70/iss4/2.

consumers from doing so. A different cost/benefit analysis is required by ex post reading, which would encourage this kind of reading because the risks and issues associated with the SFEC have already materialized.

It could be concluded by saying that reading the sophisticated long list of terms mentioned in the e-contracts are genuinely tiresome and needs changes which will not only easy to read, but also customer friendly.

Information flow between Consumer Behavior and It's Impact on E-Contract:

We are just a third of the way there when we establish that some customers examine SFECs carefully and cautiously after ex-post. The fundamental ideas of contract law and theory state that the parties establish their respective rights and obligations at the critical point known as contract formation. Customers' tardiness in identifying defects in contracts they have already signed will not alter the terms of the parties' current agreement. Above all, unless the information about transaction flows from the aggrieved consumer to the ex-ante consumers contemplating a transaction, the late recognition of biased terms will not affect the vendors' actions toward other consumers. It is important to remember this. Now, we'll list and discuss five common modes of information flow. When two consumers merge into one, information will flow from the one reviewing the SFEC ex-post to the one confronted with it ex ante. However, vendors work hard to recognize repeat customers and give them special treatment in an effort to reduce this information flow. Better contractual terms or a more accommodating "interpretation" of such terms in the event of a dispute could result from this. These tactics can obviously stop this kind of data flow.

This flow happens when the actions taken by the vendors in response to disgruntled (or satisfied) customers, which mirror the SFEC's contents, are turned into a "story" that is covered by the media. After being reported, some potential ex-ante customers learn about the

SFEC, which helps them with their ex-ante deliberations and vendor negotiations. There are serious restrictions on the flow of information. Not many stories about unfair contract clauses catch the attention of the mainstream media, which has to produce content for a wide audience with short attention spans in a highly competitive environment. Ex-post customers who are upset may find it "hard to sell" their story to the mainstream media because of their penchant for sensationalism. Informal and social channels of data distribution, like friends, neighbors, and family, can facilitate the flow of information. It can even happen between random people who coincidentally have similar experiences and interests to these customers. However, there are a number of limitations to these types of information flows. The ex ante consumer needs to engage with another person who is an ex post consumer, is aware of the relevant vendor's SFEC, and is a member of the consumer's social or professional network in order for them to be successful. These restrictions significantly reduce the likelihood that these kinds of interactions will take place. It's important to take into account the two possible ways that such a flow could start.

It may begin with an ex-post client who chooses to vent to friends and colleagues about how dissatisfied they are with a specific vendor's SFECs. For this to happen, the ex ante customer must remember the relevant information when handling a comparable transaction. To get the information they need, the ex ante consumer might also initiate this information flow by letting others know that they are interested in the information. The time and attention costs involved in this action, for both the contacting and the contacted persons, severely restrict such flows.

The use and reliance of such information by the ex-ante consumer.

This section looks at whether the information flow between the ex-post and ex-ante will be improved or perhaps slowed down in an online environment. In doing so, I consider current

technological instruments and social trends that are influenced by the Internet. Every one of the three "chokepoints" of the ex post-ex ante information flow discussed above is covered by my analysis. Consumers won't be as likely to review SFECs after they've been sold, according to an analysis of the online space. Given the nature of e-commerce, they might believe that seeking recourse is unlikely because many e-commerce vendors are geographically distant and may be difficult to get in touch with. Furthermore, the common law "caveat emptor" principle may be more closely adhered to in e-commerce markets and dynamics due to the relatively low prices that are characteristic of many online transactions. Customers will therefore be content to put up with several flaws in this situation and forego consulting their SFECs.

Online agreements are written by a single business entity, and the website operator. The majority of SFECs found online are rarely, if ever, negotiable." Additionally, online consumers could encounter a more harsh reality: offline clients can protest to the vendor's local representatives, but online users seem to be prohibited from expressing their discontent through the automated interface of the vendor." Reactions to online standard form contracting have been frantic. Online SFECs are governed by consumer protection laws that legislators have established."Courts have also been asked to rule on the enforceability of online consumer contracts and the potential for revocation of any unbalanced clauses. We now address the issue of what policy should be put in place regarding online SFECs, which academia has also been debating.

The NIA argues that SFECs will prove to be balanced and offer an effective distribution of risks and obligations when market forces are properly aligned. The same reasoning applies to online contracting. dreading the loss of marginal customers in the cutthroat B2C internet market sellers are required to create SFECs that are balanced. Additionally, the NIA easily aligns with more general concepts of Internet policy doctrine. Many have argued that this

realm should be treated as borderless and order less since the invention of the Internet. Commentators argue that since technology will soon surpass legal restrictions, regulation in this area will impede the growth of the internet. Moreover, they claim that regulations won't work because internet businesses transcend national boundaries. Notwithstanding the veracity and correctness of these claims, they nonetheless convey a potent idea that aligns with the NIA's dissatisfaction with judicial and governmental interference. The Internet market domain perfectly aligns with the analytical foundations and requirements of the NIA. Because entry barriers to online B2C markets are relatively low, competition is fierce.

Online interface, E-Contracts and Prior Informed Consent:

In today's time, we are more comfortable in shopping under the roof of our own home. We generally visit outdoor shops when either there is a big discount going on or if we need the desired item at once. I think everyone will agree with me when I say that, generally the chances of us going through the terms and conditions rises the price of that product. The more higher the cost the more higher are the chances of us reading the terms and conditions of reading the user manual and the return policy. Now, when we shop on online platforms like Amazon, Flipkart or any other service including travel and food industry we have the higher chances of coming close to the Stand form of e- contracts rather than sopping inside a physical shop. Keeping them all in mind there are several factors which actually impacts our decision making system while using on-line platforms. In this part of the chapter let us have a quick look at them. Some of the rational explanations align with barriers to reading found in the paper world, such as the relative certainty that nothing will go wrong, the lack of clarity in boilerplate, and the lack of consumer choice and bargaining power. Furthermore, the e-environment makes reading even more pointless because there is no live contracting partner and it takes time and effort to find terms that e-businesses can easily conceal. To put it briefly, e-consumers can logically weigh the advantages and disadvantages of reading terms

and determine that it would be better to use their time for something else[190]. The e-environment seems to benefit e-consumers at first glance since it removes social pressures like pushy salespeople and impatient customers in line. It will be important to note that reading and understanding terminology in the e-environment presents extra challenges. Electronic consumers might not recognize the gravity of their actions because they are unable to assign the proper importance to a mouse click[191]. Furthermore, it seems that a lot of consumers are under the influence of computers and the Internet, which makes them impulsive and impatient. It can be said that the behavior of many customers considers e-standard e-forms as "click-happy" behavior[192].

The legislation connected with mandatory disclosures varies country to country. For instance, during the trade war between USA vs. China, India had forced its e-market players to disclose the Country of origin of the products, which they were offering to Indian Customers. Many will say that as India was eyeing to snatch the 'Global manufacturer' tag from China using the opportunity provided by Chinese Covid-19, we shall rather take it as India's baby steps towards creating a strong "Privacy" regime. To explain it further, let us further discuss about Indian Individual importers behavior while importing foreign goods. Prior to Ban of Chinese Apps, we are used to create online profiles in various Chinese websites like Ali baba, and we used to share our residential, financial data with Chinese stake holders. Sheldom, we used to check the "Privacy" policy of such App and have never thought of any kind repercussions which may have been inflicted upon us. Another instance of such "Privacy" violation was during online loan App Scandal. During the mid 2021-22, specifically when the common men were struggling to recover from Chinese Covid-19, at that time Chinese APPs were running the online loan business. The business model was very simple, the applicant has

[190] Gerhard Wagner, *The Dispute Resolution Market*, 62 BUFFALO LAW REVIEW.
[191] Robert A. Hillman, *Online Boilerplate: Would Mandatory Website Disclosure of E-Standard Terms Backfire?*, 104 MICHIGAN LAW REVIEW 837 (2006).
[192] Wagner, *supra* note 24.

to upload their identification details such as the Voter ID, Pan Card and Adhar Card on that App and after verification they will get the desired amount. Everything was fine till this extent, however after sometime the agents of that loan app used to torment the victims for quick payments of loan money. They used to send scandalous threats on the borrower's phone as well as on the other people who were connected to the borrowers. This led to serious violation of "Privacy" by the loan apps and the legislators had to take quick initiatives to block such uninvited "Privacy" invasions.

After these incident, the legislators focused on Mandatory disclosure on e-platforms so that Indivials can be more alert while sharing private information on such platforms.

The Pros of Mandatory Disclosure by E-Platforms:

Theoretically, e-disclosure requirements would drive up the number of people who read standard forms and shop for terms to a point where companies could no longer afford to ignore them. Mandatory website disclosure would also enable buyers to educate themselves by examining and contrasting terms at a distance from the thrill and expectation of a near future transaction. Companies in markets with intense competition would fight for a bigger market share by crafting phrases that appeal to customers. Companies in less cutthroat sectors would try to write catchy headlines to draw in as many readers as possible[193]. Customers could shop in these markets with a certain level of assurance that the terms' quality would be suitably reflected in the prices[194].

In theory, mandatory website disclosure could still encourage companies to write fair terms even if it had little effect on consumer reading. Companies might be concerned, for instance,

[193] Becher, *supra* note 13.
[194] Dangerous Terms: A User's Guide to EULAs, ELECTRONIC FRONTIER FOUNDATION (2005), https://www.eff.org/wp/dangerous-terms-users-guide-eulas (last visited Feb 11, 2024).

that disclosure would allow watchdog groups to reveal offensive language[195]. Such exposure could destroy a company's reputation, which is particularly important on the internet where customer trust is essential to success, and consequently reduce the company's market share. For example, when you are willing to write a positive review regarding any products on e-platforms, they will always welcome you. However when you would want to write a critical review, they will not allow you to do so without scrutinizing it first. I say, that's the violation of my freedom of-speech. An we are all aware that Right o "Privacy" and "Freedom of Speech" both forms a part of Right to Life, enshrined in "Article 21 of Indian Constitution". Contract law would support autonomy justifications for contract enforcement by expanding the ability to read e-standard forms. When given the chance to read and compare terms, consumers are better equipped to decide whether and with whom to enter into a contract.

Standard forms should be inexpensive to display on a website, so the obvious costs of requiring website disclosure shouldn't be too high. In actuality, businesses haven't been able to present a convincing case against the requirement up to this point[196]. Legislators shouldn't encounter insurmountable difficulties when creating regulations that effectively incorporate disclosure. If e-businesses are to be discouraged from creating strategies to hinder reading, the regulations governing mandatory website disclosure need to be explicit and comprehensive. Plain English language that is easily readable on a website's home page or via a prominently marked hyperlink may draw in more visitors than legalese which requires multiple mouse clicks[197]. Therefore, mandatory website disclosure laws must take these tactics into consideration by mandating that companies display terms on their homepages or

[195] Christian J. Meier-Schatz, *A Fresh Look at Business Disclosure*, 51 THE AMERICAN JOURNAL OF COMPARATIVE LAW 691 (2003).
[196] Juliet M Moringiello & William L Reynolds, *What's Software Got To Do with It? The ALI*, 84 TULANE LAW REVIEW.
[197] Gary M. Olson & Judith S. Olson, *Human-Computer Interaction: Psychological Aspects of the Human Use of Computing*, 54 ANNU REV PSYCHOL 491 (2003).

on a page that is only accessible through a few clicks. Moreover, scroll-down windows that vanish or are too small should be prohibited by the rules.

The cost of establishing that a company did not, or did not display its terms prior to the transaction in a way required by law, would be included in the enforcement costs. Mandatory website disclosure laws might place the onus of proving the content of websites on businesses, encouraging them to maintain accurate records of their content. Currently, a lot of online businesses maintain archived copies of their website content, which include the dates of its introduction, modification, and removal. Additionally, they keep track of server logs, which show when and if a webpage was altered. Every e-business would have to comply with a system of required website disclosure. Of course, companies that are willing to commit fraud might be able to change their records, but this issue shouldn't be all that dissimilar from the difficulty of rooting out fraud in the paper contracting industry. The testimony of other website users during the disputed period, for instance, could serve as evidence to support a business's claims. By looking through their web logs, e-businesses can locate these visitors. In the online realm, we can anticipate that as technology develops quickly and as entrepreneurs take their ideas forward, new techniques for proving website content over time will also be created. For instance, don't be shocked if new websites appear to archive the common e-business models if contract law adopts mandatory website disclosure.

Standard form of E-Contract- Their mandatory Disclosure and its Risks for Economy:

More people than ever before are considering data “Privacy” to be a serious issue; some have even declared it to be a human rights one. The majority of nations have implemented consumer protection laws that control the gathering, storing, and use of data. Businesses are responsible for making sure there are no infractions. Because e-commerce is a digital business, “Privacy” policies are especially important. E-commerce “Privacy” policies ought

to be transparent about the collection, storage, use, and sharing of data. This covers every detail, including phone numbers, credit card details that have been saved, past purchases, and interactions with advertisements. 75% of consumers worldwide will be subject to "Privacy" regulations by 2023[198]. This implies that to comply with legal requirements and safeguard the data of clients, staff members, and partners, e-commerce websites need to have procedures and safeguards in place.

E-Commerce is the focus of mandatory website disclosure, which only enforces terms that are present on a company's website before a transaction. Naturally, the terms themselves are not required to comply with this rule. With the hope that more customers will read and search for terms, or that watchdog organizations will make negative terms public, disclosure is meant to persuade companies to write reasonable terms[199].

Currently many Developed, Developing countries have developed their own e-commerce regulation to protect "Privacy" of their own citizents. Let us have a quick look at them:

- **Consumer "Privacy" Act of California (CCPA)[200].**

The most extensive data "Privacy" law enacted at the state level is the CCPA. California law requires businesses that gather personal data about their clients to provide a clear notice of the data they collect, as well as the option to have it deleted at their request. The state's first "Privacy" law, the California Online "Privacy" Protection Act (CalOPPA), is in addition to this.

[198] Study predicts "Privacy" laws will regulate 75% of worldwide consumers by 2023, https://iapp.org/news/a/gartner-predicts-75-of-consumers-will-fall-under-"Privacy"-laws-by-2023/ (last visited Feb 11, 2024).
[199] Efthymios Constantinides, *Influencing the Online Consumer''s Behaviour: The Web Experience*, INTERNET RESEARCH (2002).
[200] California Consumer "Privacy" Act (CCPA) | State of California - Department of Justice - Office of the Attorney General, https://www.oag.ca.gov/"Privacy"/ccpa (last visited Feb 11, 2024).

- **California “Privacy” Rights Act (CPRA)[201]**

The CPRA expands upon the CCPA by granting users the ability to limit how personal information is used, update inaccurate data, and set storage time limits for specific types of information.

- **Virginia's Consumer “Data Protection” Act (C”DPA”)[202].**

The General “Data Protection” Regulation act of the European Union and Virginia's CCPA are somewhat similar. Businesses that sell to Virginians are required to provide opt-in options for personal information.

- **Colorado “Privacy” Act (CPA)[203].**

Colorado is the third state to enact legislation pertaining to data “Privacy”, drawing from earlier legislative efforts. It includes the ability to remove information, find out what data has been collected, and choose not to receive targeted advertisements.

- **New York SHIELD Act[204]**.

Laws pertaining to the security of personal information are included in the broader set of consumer protections provided by the Stop Hacks and Improve Electronic Data Security (SHIELD) Act.

- **Connecticut's law on data “Privacy”[205]**.

---

[201] California “Privacy” Rights Act, WIKIPEDIA (2024), https://en.wikipedia.org/w/index.php?title=California_”Privacy”_Rights_Act&oldid=1199231267 (last visited Feb 11, 2024).
[202] Code of Virginia Code - Chapter 53. Consumer “Data Protection” Act, https://law.lis.virginia.gov/vacode/title59.1/chapter53/ (last visited Feb 11, 2024).
[203] Colorado “Privacy” Act (CPA), CONSUMER “PRIVACY” ACT, https://www.consumer”Privacy”act.com/colorado-”Privacy”-act-cpa/ (last visited Feb 11, 2024).
[204] SHIELD Act | New York State Attorney General, https://ag.ny.gov/resources/organizations/data-breach-reporting/shield-act (last visited Feb 11, 2024).
[205] The Connecticut Data “Privacy” Act, CT.GOV - CONNECTICUT’S OFFICIAL STATE WEBSITE, https://portal.ct.gov/AG/Sections/”Privacy”/The-Connecticut-Data-”Privacy”-Act (last visited Feb 11, 2024).

The law from Connecticut has taken effect on July 1, 2023, and is applicable to any organization that owns or controls personal data.

- **The GDPR of the EU[206].**

The GDPR serves as the foundation for much of the current data "Privacy" rules. It is the most extensive rule that has been passed thus far and serves as the foundation for most subsequent "Privacy" legislation. Included are restrictions on the use of data, rights to be informed of "Data Breach"es, and safeguards for consent.

- **The Electronic Documents and Personal Information Protection Act (PIPEDA) of Canada**[207].

Canada's "Privacy" protection legislation was actually initially passed in 2000 and has been amended several times to keep it up to date with changes in the use of data.

- **The General Law of Personal "Data Protection" in Brazil (LGPD)[208].**

According to the GDPR, Brazilian law is applicable to all Brazilian nationals, regardless of whether a business is headquartered there.

One may ask, despite having so much legislations in hand, why can't we protect our "Privacy" from potential risk of loss of "Privacy". Well, the answer to this question will be full of sarcasm. For instance, the new guidelines proposed by the NGT, where it is mentioned that upon taking necessary permission from NGT, manufacturers can establish their factories in protected forest land as well. This legislation was originally intended to protect Forest

[206] General "Data Protection" Regulation, WIKIPEDIA (2024), https://en.wikipedia.org/w/index.php?title=General_Data_Protection_Regulation&oldid=1203651507 (last visited Feb 11, 2024).
[207] Office of the "Privacy" Commissioner of Canada, *The Personal Information Protection and Electronic Documents Act (PIPEDA)*, (2021), https://www.priv.gc.ca/en/"Privacy"-topics/"Privacy"-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/ (last visited Feb 11, 2024).
[208] General Personal "Data Protection" Law, WIKIPEDIA (2024), https://en.wikipedia.org/w/index.php?title=General_Personal_Data_Protection_Law&oldid=1205648883 (last visited Feb 11, 2024).

Land, however by taking advantage of the loop holes in the legislation many has bent the law in their favor. Similarly, as the data “Privacy” legislations are comparatively new to the legislators, it will take more time to create a wholesome legislation to protect “Privacy” of consumers on E-commerce websites.

Coming back to our original discussion as previously mentioned, since watchdog organizations can publicize unjust terms, requiring website disclosure may encourage companies to write reasonable terms. The issue is that, while the threat of watchdog groups may incentivize companies to refrain from drafting outrageous terms, it might not be enough to stop them from drafting terms that would negatively impact consumers' perceptions even though they might not raise major red flags. For instance, a company that is concerned about watchdog groups might avoid including a clause requiring a customer to pay the company's legal fees and costs in any case or to arbitrate in a non-neutral forum. However, these clauses may still be unenforceable due to its unforeseen nature. However, a company may determine that the advantages of a forum-selection clause that causes inconvenience to the customer or a clause that permits an online platform to "collect certain non-personally identifiable information about a consumer's web surfing and computer usage" outweigh the costs of any negative publicity they may generate.

Mandatory website disclosure may have the unintended consequence of giving businesses a safe haven to use derogatory but appropriate language. Conditions that were previously deemed unconscionable or related may still be enforceable due to their reasonable disclosure[209]. Both procedural and substantive unconscionability are sought in the majority of cases involving unconscionability or related claims, including those involving e-

[209] Comb v. Paypal, Inc., 218 F. Supp. 2d 1165 | Casetext Search + Citator, https://casetext.com/case/comb-v-paypal-inc-2 (last visited Feb 11, 2024).

commerce[210]. Procedural unconscionability refers to the circumstances surrounding the contract's formation and governs scenarios that bear similarities to duress, misrepresentation, or most importantly in this case an unfair representation of the terms. Although substantive unconscionability focuses on whether an exchange is egregiously imbalanced, contract law typically does not assess the suitability of an exchange[211]. Many courts use a sliding scale in their unconscionability investigations, stating that "less evidence of procedural unconscionability is needed to conclude that a term is unenforceable the more substantially oppressive the contract term, and vice versa."[212]

"Privacy" Management:

The advent of Big Data and fusion centers, data security breaches, the rise of Web 2.0, rising marketing, and the expansion of monitoring technology have all exacerbated "Privacy" issues during the last decade. Policymakers in developed and developing countries have proposed and passed substantial new regulations, but the underlying approach to preserving "Privacy" has remained largely intact since the 1970s. The law currently offers people some rights that allow them to decide how to manage their data. These rights essentially include the rights to be notified, to access, and to consent to the collection, use, and disclosure of personal data. The purpose of this set of rights is to provide people control over their personal data, so that they can balance the costs and benefits of the acquisition, use, or disclosure of their information for themselves. In this era of e-consent management of "Privacy" is very important. Let us discuss what issues one individual may face during managing their consent and managing their "Privacy".

[210] Robert A Hillman, *Debunking Some Myths About Unconscionability: A New Framework for U.C.C. Section 2-302*, 67 CORNELL LAW REVIEW.
[211] Hillman, *supra* note 9.
[212] *Armendariz v. Foundation Health Psychcare Services, Inc.*, WIKIPEDIA (2023), https://en.wikipedia.org/w/index.php?title=Armendariz_v._Foundation_Health_Psychcare_Services,_Inc.&oldid=1175138606 (last visited Feb 11, 2024).

A. Analytical Problems: crucial aspects of “Privacy” management consist of notifying individuals about the data collected and used about them (notice) and allowing them to choose whether or not to accept such collection and use (option). By giving “Privacy” notices and the option to opt out of some of the forms of data collection and use indicated in the notices, entities have normalised the practise of providing notice and choice. In the United States, the FTC has stepped in to enforce “Privacy” notifications. Since 1998, the Federal Trade Commission has maintained that breaching “Privacy” notice commitments constitutes "unfair or deceptive acts or practices in or affecting commerce" in violation of the Federal Trade Commission Act. When the FTC discovers such a breach, it has the authority to file civil cases and seek injunctive relief. The method of notification and choice has also been a focal point of “Privacy” regulation. For example, the Gramm-Leach-Bliley Act (GLBA)[213] mandates financial institutions to give clients with “Privacy” notifications and to let them to opt out of data sharing with third parties. People do not appear to be engaged in much “Privacy” management, despite their embracing of notice and choice. The vast majority of consumers do not read “Privacy” notifications on a regular basis[214]. Studies reveal that just a small fraction of individuals read other sorts of notices, such as end-user license agreements and contract boilerplate terms. Furthermore, when given the option, few people choose not to

[213] 2 Pub. L. No. 106-102, 113 Stat. 1338 (codified in scattered sections of 12 and 15 U.S.C).

[214] 4 See Helen Nissenbaum, “Privacy” in Context 105 (2010) (discussing a 2006 study showing that only 20% of people read “Privacy” notices "most of the time" (quoting TRUSTe & TNS, Consumers Have a False Sense of Security About Online “Privacy”: Actions Inconsistent with Attitudes, PR NEWSWIRE, http://www.prnewswire.com/news-releases/consumers-have-false-sense -of-security-about-online-”Privacy”—actions-inconsistent-with-attitudes-55969467.html (last visited Sept 29, 2023) (internal quotation marks omitted))); Fred H. Cate, The Failure of Fair Information Practice Principles, in consumer PROTECTION IN THE AGE OF THE 'INFORMATION ECONOMY' 343, 361-62 (Jane K. Winn ed., 2006); George R. Milne & Mary J. Culnan, Strategies for Reducing Online “Privacy” Risks: Why Consumers Read (or Don't Read) Online “Privacy” Notices, 18 J. INTERACTIVE MARKETING 15, 20-21 (2004) (finding that only 4.5% of respondents said they always read website “Privacy” notices and 14.1% frequently read them)

have their data collected, used, or disclosed[215]. The majority of individuals do not bother changing the default "Privacy" settings on websites.

People do not appear to be engaged in much "Privacy" management, despite their embracing of notice and choice. The vast majority of consumers do not read "Privacy" notifications on a regular basis. Studies reveal that just a small fraction of individuals read other sorts of notices, such as end-user license agreements and contract boilerplate terms. Furthermore, when given the option, few people choose not to have their data collected, used, or disclosed. The majority of individuals do not bother changing the default "Privacy" settings on websites[216]. A more difficult issue occurs when ideas for improved notice, whether simplified or more obvious, are proposed. Such techniques neglect a fundamental usage of notice: keeping things simple and easy to understand clashes with thoroughly informing people about the consequences of disclosing data, which are pretty difficult to understand if presented in sufficient detail to be meaningful. People need a greater understanding and background to make informed decisions. However, many "Privacy" notices are vague about potential future data usage. Furthermore, if people wants to read and understand the terms and condition they are not usually allowed to do so. For example, if you want to unsubscribe any services online, the service provider will start redirecting you to countless subsidiary websites and make it more complex.

B. Making unreasonable decision: Even if most people read "Privacy" policies on a regular basis, they frequently lack the experience to fully assess the ramifications of agreeing to specific present uses or disclosures of personal data. People often hand out their data for

[215] Omri Ben-Shahar & Carl E. Schneider, The Failure of Mandated Disclosure, 159 U. PA. L. Rev. 647, 665-78 (2011); Florencia Marotta-Wurgler, Will Increased Disclosure Help? Evaluating the Recommendations of the ALI's "Principles of the Law of Software Contracts," 78 U. chi. L. Rev. 165, 178 (2011) (discussing a study that revealed that people accessed contract boilerplate terms far less than 1% of the time).

[216] ee M. Ryan Calo, Against Notice Skepticism in "Privacy" (and Elsewhere), 87 NOTRE DAME L. Rev. 1027, 1033 (2012) ("Studies show only marginal improvement in consumer under standing where "Privacy" policies get expressed as tables, icons, or labels, assuming the consumer even reads them")

insignificant rewards[217]. Some draw the conclusion that consumers place little value on "Privacy". Some argue that there is a generational shift in "Privacy" norms, with young people not caring about "Privacy". However, people consistently declare how much they value "Privacy" in surveys, and attitudes towards "Privacy" among the young and old are, unexpectedly, relatively similar[218].

Conclusion:

The amount of digital data is growing exponentially, which presents new difficulties for criminal and national security investigations. There is a conflict between the necessity of digital data for these kinds of investigations and the requirement to uphold a nation's sovereignty to safeguard its citizens' "Privacy". Any approach to overcoming these obstacles must also account for the urgency with which information is required for criminal or national security investigations, as well as the possibility that the information may be difficult to find. A fundamental human right is "Privacy", and computer systems hold a lot of potentially sensitive data. The Information Technology Act's Chapters IX and XI outline the consequences for violating data "Privacy" and confidentiality in relation to illegal access to computers, computer systems, computer networks, data destruction, duplication, or transmission, computer databases, etc. Financial data, health data, business proposals, intellectual property, and sensitive data may all be covered by "Data Protection". Today, though, information related to anyone can be accessed at any time and from any location, which presents a new risk to private and sensitive data. Globalization has made technology

[217] Alessandro Acquisti & Jens Grossklags, "Privacy" and Rationality: A Survey, in "Privacy" and technologies OF Identity is, 16 (Katherine J. Strandburg & Daniela Stan Raicueds., 2006)

[218] Chris Jay Hoofnagle et al., How Different Are Young Adults from Older Adults When It Comes to Information "Privacy" Attitudes & Policies? (Aug. 14, 2010) (unpublished manuscript) available at http://papers.ssrn.com/s0l3/papers.cfmPabstract_ids 1589864

more widely accepted. Different nations have periodically introduced new legal frameworks in response to growing demands, such as the UK's “Data Protection” Act of 1998 and the USA's Electronic Communications “Privacy” Act of 1986. In the United States, there are specific “Privacy” laws that safeguard individual medical records, children's online “Privacy”, private financial information, and student education records. Self-regulatory initiatives are helping to define better “Privacy” environments in both countries. With its pervasive surveillance, the 5G era offers the possibility of significant losses in terms of safety, anonymity, “Privacy”, and general well-being in addition to the promise of actual economic gains. The majority of the “Privacy” concerns covered in this report, if not all of them, exist before the 5G era but will only intensify as 5G is deployed. Although it can be difficult, juggling demands that are valid but frequently at odds with one another seems like a good idea. Furthermore, we think it can be accomplished in a way that proves the validity of the outcome and results in a long-lasting conclusion to this competition. Revenue is crucial, but it shouldn't be the sole indicator used to evaluate technology. All things considered, requiring website disclosure might still be the most effective way to address the issue of e-standard forms. As previously stated, alternative solutions come with a number of serious drawbacks. Furthermore, requiring website disclosure is inexpensive, supports the assertion that consumers gave their consent, and represents a symbolic win for proponents of increased equity in e-standard-form contracts. Of course, these arguments for mandatory website disclosure are only compelling if my concern about a potential legal backlash turns out to be unfounded, as the advantages of disclosure exceed the expenses of enforcing certain dubious terms.

CHAPTER 6

Conclusion and Suggestions:

“Privacy” stands as a cornerstone of individual autonomy, dignity, and freedom within any society governed by the rule of law. As we conclude our exploration of “Privacy” as an essential component of constitutional rights, it becomes evident that its recognition and protection are indispensable in safeguarding the inherent liberties of citizens. Throughout this analysis, we have delved into the historical context, legal frameworks, and contemporary challenges surrounding “Privacy” within constitutional contexts. Any country's Constitution is its foundational legal document, outlining the rights and obligations of its citizens as well as the guiding principles that form the basis of its governance. Similarly, Within the framework of the Indian Constitution, the right to “Privacy” is an essential pillar that upholds the core principles of liberty, autonomy, and dignity of the Indian Citizens. The Indian judiciary's acknowledgment of it as an essential component of personal liberty has greatly improved citizens' defences against unauthorized intrusions by both state and non-state entities. The development of the right to “Privacy” within Indian law is a reflection of both the judiciary's dedication to upholding human rights in the digital era and the changing character of constitutional interpretation. The Supreme Court of India has reaffirmed the right to “Privacy” as a “fundamental right”, necessary for the maintenance of individual autonomy and dignity in a contemporary democratic society, with historic rulings like the Puttaswamy case. Although the term "“Privacy”" does not appear explicitly in the US Constitution, the judiciary has interpreted it to include the right to “Privacy” based on the penumbras and emanations of several amendments, most notably the First, Fourth, Fifth, and Fourteenth. This interpretive method recognizes that constitutional law is dynamic and that it is necessary to modify core ideas to reflect modern circumstances. In India, the right to “Privacy” is

fundamental to democracy and human dignity because it protects people from unjustified interference and gives them the autonomy to manage their personal data and preferences. Fostering a free, just, and inclusive society in which each citizen's inherent worth and autonomy are respected and upheld requires its continuous recognition and protection. Indian courts have repeatedly emphasized the need to protect consumer “Privacy” and data. Consumer “Privacy” and data security are at risk from trending e-commerce. A right-based strategy is required to protect people's online “Privacy” when it comes to their data. No law in India guarantees an individual's “Privacy” or the protection of their data. Even though India's judiciary develops “Privacy” rights on a case-by-case basis, comprehensive legislation is still required as soon as possible to effectively combat. The problems with jurisdiction, choice of law, and gray areas in our current legal system must be resolved by an effective and outcome-oriented legal and regulatory framework. The traditional methods we used to handle these problems are becoming increasingly antiquated due to the growth of e-commerce. Concerns for online consumers have also changed as a result of popular e-commerce. E-contracts are essential for determining the choice of law between parties engaged in electronic commerce because they allow for the direct determination of the parties' responsibilities and obligations as well as the straightforward application of applicable laws. However, because there are at least three parties involved from separate jurisdictions who are subject to three separate legal systems, the case is not simple. Choosing which law to apply in the end is very important. Without comprehensive, internationally recognized cyber laws, these problems will keep coming up one after the other. In e-commerce, jurisdiction and choice of law are violated.

In the Era of fastest internet, we have to acknowledge the fact that ‘Being On-line’ is the present and it is going to be the future of every single economy. We cannot deny the fact that in todays world If you want to reach every single doorstep with your product, you have to

have internet and you have to ensure that you reach your customers with your product but without damaging their “Privacy”. Two years ago, Chinese Covid Virus came to India, it actually opened the door to digitalisation of Indian market. With every digital payment made through UPI or any other third party APP, India progressed a step further on it’s journey towards a Multi trillion Dollar Economy. With every single step towards a progressive society India felt the need of a strong, robust and sui-generis protective legislation. As internet has reached our bed-room no, this is the right time for enacting such legislation. Individuals demand their “Privacy”, whether consciously or unconsciously. Even though it is widely acknowledged that this right is a fundamental human right, defending one is difficult. It is challenging to assert this right because there is no agreed-upon definition. The notion of “Privacy” is subject to variation among individuals and across national borders. The “Privacy” and protection of people's data have been compromised since the advent of technology. Everyone has a natural desire to draw boundaries and defend their “Privacy” from other people and, in certain situations, the government.

The laws currently in place are ineffective at resolving legal disputes pertaining to the use of computers and the internet, and they do not address these legal issues. The safeguarding of personal information is another complex legal matter. If the person in possession of the data is careless when using the internet, he might even lose his rights over it. India lacks the appropriate legislation to handle “Privacy” and data-related concerns in the context of the expanding trend of electronic commerce. Increased use of the internet for various purposes exposes users' data, and personal information entering India through cross-border traffic is completely unprotected. To keep track of all the data that comes in and out, India needs guidelines on trans-border flows of personal data similar to those set forth by the OECD in Trans-border Flows of Personal Data 1980. India must now enact laws protecting “Data Protection” and “Privacy” in the online sphere, according to the internet community.

The First objective of my research was to study the importance of acknowledging right to "Privacy" in cyberspace as a "fundamental right". Upon completing my analysis I am of the considered opinion that the law makers may take up this matter with great concern as Indian judiciary through their judicial activism has made it clear that 'Right to "Privacy"' enshrines in article 21. If it can be a part of Art. 21, there is no harm to designate it by acknowledging it as a part of "fundamental right" in black and white.

The Second Objective of my Study was to study the prospects of a state regulatory regime defining the rights and liabilities of netizens and cyber world stake holders. Upon completing my analysis I have come to conclusion that in the world of data both the data fiduciaries/ the data service providers and the customers has to be very cautious about how would they handle their data. They has to be very vigilant about how much access they will provide to other players of their industries to use the customer data and what methods will they employ to ensure safety of that data.

The Third objective of my study was to Study the liability of cyberspace stakeholders towards protection of individual personal data at cyberspace. Upon completing my analysis I have reached the conclusion that, it is very important to determine the scale of liability of a data fiduciary in case of a breach in their system. While the developed economies has adjusted their legal system according to their citizens need, India has also spread her wings to protect her citizens from any kind of unwanted incident. India has enacted the "DPDP Act" and have updated the Information Technology Act to check the Data Fiduciaries from participating any kind of ill activities. I would like to include that with the "DPDP Act", the legislators must also empower the lower courts to take cognizance of such "Data Breach"es and inflict heavy fines against the "Data Breach"ers.

The Fourt objective of my study was to study the need of establishing mandatory international minimum common standard to protect right to "Privacy" in cyber world, irrespective of territorial jurisdiction. By now we have understood that data knows no border and data has the capacity to travel faster than our thoughts. In such a fast world global legislators must come forward in a joint manner and create an uniform law which will function domestically and internationally. One may ask, given the factors like different nation different law, will this Idea actually work. Well, if GDPR can be successful than IDPR (International "Data Protection" Rules) can become successful.

The Last and Final objective of my study was to Study the concept of "Right to be forgotten" and analyze the importance of the concept in context to Right to "Privacy". "Right to be forgotten" is a new concept in India and has found a considerable amount of foot-hold in our Country. With the spread of Internet, nothing is truly private anymore, anyone can access our data and share it with rest of the world. In a given scenario where our personal information has been leaked, we will definitely want to secure those information and take it down from the Internet. A year back this seemed to be impossible, fortunately the "DPDP Act" has come to its rescue and has acknowledged the Need of Erasing Unwanted Data from the WWW. Anywebsite.com.

I would like share some of my own inputs under the umbrella of "suggestions' for the future readers and Policy framers, so that it may assist them in their journey of framing a Global "Data Protection" Legislation.

1. **Broadening the Sphere of Right to Life, by considering 'Right to "Privacy"' as an Integral part:**

   If there is no "Privacy", can we enjoy our Right to life? I am sure most of us will agree that, we cannot enjoy our right to life if there is no "Privacy". Policy framers

have understood the importance of right to “Privacy”, and now it is the high time to consider to include ‘Right to “Privacy”’ as part of constitutional as well as “fundamental right”.

2. **Data fiduciaries should be liable to store data of a particular nation inside that nation’s territory:**

   The Information Technology Act of 2008, the Indian Penal Code of 1806, the Indian Evidence Act, the Indian Contract Act, the Code of Civil Procedure, the Consumer Protection Act, the SEBI guidelines, and the R.B.I. guidelines are all available in India; however, no matter how they are read or codified, they will not be able to address “Privacy”-related issues. India's data “Privacy” and security problems stem from a patchwork of laws. The basic reason why the traditional laws are ineffective in addressing these two problems in e-Commerce platforms is that while the internet is dynamic, these Acts are not. When parties from different jurisdictions engage in e-commerce transactions, these two issues become even more serious. The principles of jurisdiction impose boundaries on consumers and courts worldwide, while the internet has no boundaries. The question of choice of law, choice of forum, and choice of jurisdiction arises in such situations. The other issues that must be resolved as soon as possible are which laws will apply to the parties and whether the court's decision will be enforceable against them. If lawmakers do not pass a “Privacy” and data law that defines “Privacy” and data “Privacy” and is sufficiently comprehensive to address issues related to “Data Protection” and the penalties for “Data Breach”es, this problem will persist.

3. **The process of data mining, data transportation should be transparent:**

   Do I know, where I am being stored digitally? It means that A customer of data fiduciaries must have a clear idea about the place where his data is being stored by the

service providers. In India we still don't have the infrastructure to determine the liabilities of a "Data Breach"er if he is running his business beyond the territorial jurisdiction of india. To ensure proper safety of the data, the data fiduciaries must be made liable to store their data inside the territorial jurisdiction of India and the customer must be informed about the whereabouts of his data. This way transparency as well as the need of proper prior informed consent requirement will be satisfied.

4. **The Law enforcement agencies should be given proper training so that they can be technologically sound to tackle issues related to cyber security.**

It is said that Pen is mightier than the sword. However in today's world we need the sword to protect others from the pen. Except metro cities, the law enforcing authorities are not properly trained to handle issues related to Data "Privacy" breach. Many studies shows that Indian police stations are not equipped with proper machineries or training to handle cyber crimes properly. So, proper training should be organised and they should be given in-hand practical experience to tackle such issues.

5. **Introduction of Self Data Management system:**

One person can manage their data on their own, provided he has the necessary information regarding how to manage it and has the back up from their domestic legislation. Hence sensitization on "Privacy" and data management is the need of the hour.

6. **Laws governing the trans-border flow of data:**

The internet makes it possible for data to move quickly between jurisdictions. Such information may include sensitive and private information about a person's health,

financial accounts, preferences, and other topics. Without legislation to regulate the transfers of data between jurisdictions, there would be confusion and a loss of track of the data. In the era of the internet, it is customary for people to divulge personal information to use online services, and failing to do so may result in their account being blocked. Every service made possible by an online platform should include a "consent option" and brief details about the safety measures taken by the service providers to ensure the security of the data.

7. **Children's online "Privacy" law:**

Children are the worst victim of online cyber bullying and breach of "Privacy". Most of the children are not aware about their rights and seldom know where to find proper help for any issues related to the internet. The Indian government needs to take the lead in drafting a separate online "Privacy" law for kids who use Face book, Instagram, Tiktok and other personal messaging services. Like the "U.S. COPPA Act" of 1998, the Act must seek to regulate the transfer of their personal information.

8. **Sensitization of data producers and Observation of vigilance in the field of cyber space:**

Given the growing threat of cybercrimes, I would recommend requiring all data service providers to participate in an awareness program about crimes committed via the use of computers and the internet. Additionally, I would urge them to speak with a police officer about forming a committee so they can coordinate their efforts to take down cybercriminals. Maintaining an aerial perspective of the clientele is imperative.

I would like conclude the thesis by mentioning that the world can not run without Data, for the benefit of this civilization Data is the most important ingredient. It is our

duty today to ensure that our data is well protected and well used for shaping our future.

I would like conclude the thesis by mentioning that the world can not run without Data, for the benefit of this civilization Data is the most important ingredient. It is our duty today to ensure that our data is well protected and well used for shaping our future.

Bibliography:

References:

Books:

- Seervai H.M, Constitutional Law of India, Universal Law Publishing (2015)
- D.D. Basu, Comparative Constitutional Law, LexisNexis (2014)
- Michael Chertoff, Exploding Data: Reclaiming Our Cyber Security in the Digital Age, Black Cat Publications (2019)
- Andrew T. Kenyon and Megan Richardson, New Dimensions in Privacy Law: International and Comparative Perspectives, Cambridge University Press (2006).
- Dara Hallinan(ed) "et al", Data Protection and Privacy, Bloomsbury Publishing (2021).
- Franz Werro (ed), The Right To Be Forgotten, Springer publication 2020.
- Meg Leta Jones, Ctrl + Z: The Right to Be Forgotten, New York University Press 2018.
- Punit Bhatia and Eline Chivot , AI & Privacy: How To Find Balance, Independent Publication, 2021.
- Samuel D Warren "et al", The Right to Privacy, Quid Pro, LLC (2015).

Articles:

- Atul Singh, DATA PROTECTION: INDIA IN THE INFORMATION AGE, 59 Journal of Indian Law Institute 78–101 (2017), https://www.jstor.org/stable/26826591.
- Christiane Wendehorst, Strict Liability for AI and other Emerging Technologies, 11 Journal of European Tort Law 150– 180 (2020), https://www.degruyter.com/document/doi/10.1515/jetl-2020-0140/html.
- Jed Rubenfeld, The Right of Privacy, 102 HARVARD LAW REVIEW 737–807 (1989), https://www.jstor.org/stable/1341305.
- Jerry Kang, Information Privacy in Cyberspace Transactions, 50 Stanford Law Review 1193 (1998), https://www.jstor.org/stable/1229286?origin=crossref
- Julia Carrie Wong, The Cambridge Analytica scandal changed the world – but it didn't change Facebook, The Guardian, March 18, 2019, https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-theworld-but-it-didnt-change-facebook.
- Judith Jarvis Thomson, The Right to Privacy, 4 Philosophy & Public Affairs 295–314 (1975), http://www.jstor.org/stable/2265075.
- Kristian P. Humble, International law, surveillance and the protection of privacy, 25 The International Journal of Human Rights 1–25 (2021), https://www.tandfonline.com/doi/full/10.1080/13642987.2020.1763315.
- M. T. Dlamini et al., Digital deception in cybersecurity: an information behaviour lens (2020), http://informationr.net/ir/25-4/isic2020/isic2018.html

- Monique Mann et al., The limits of (digital) constitutionalism: Exploring the privacy-security (im)balance in Australia, 80 International Communication Gazette 369–384 (2018), https://doi.org/10.1177/1748048518757141
- Nir Kshetri, Blockchain's roles in strengthening cybersecurity and protecting privacy, 41 TELECOMMUNICATIONS POLICY 1027–1038 (2017), https://linkinghub.elsevier.com/retrieve/pii/S0308596117302483
- Paul Voigt & Axel von dem Bussche, The EU General Data Protection Regulation (GDPR) (2017), http://link.springer.com/10.1007/978-3-319-57959-7
- Raymond Bierens, Bram Klievink & Jan van den Berg, A Social Cyber Contract Theory Model for Understanding National Cyber Strategies, 10428 in Electronic Government 166–176 (Marijn Janssen et al. eds., 2017), http://link.springer.com/10.1007/978-3-319-64677-0_14
- Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, Harvard Law Review 193–220 (1890), https://www.jstor.org/stable/1321160.
- Scott J. Shackelford, Scott Russell & Andreas Kuehn, Defining Cybersecurity Due Diligence Under International Law: Lessons from the Private Sector, in Ethics and Policies for Cyber Operations 115–137 (Mariarosaria Taddeo & Ludovica Glorioso eds., 2017), http://link.springer.com/10.1007/978-3-319-45300-2_8
- Yanfang Wu "et al", A comparative study of online privacy regulations in the U.S. and China, 35 TELECOMMUNICATIONS POLICY 603–616 (2011).
- "Privacy" Law in India: A Muddled Field - I — The Centre for Internet and Society, https://editors.cis-india.org/internet-governance/blog/the-hoot-bhairav-acharya-april-15-2014-"Privacy"-law-in-india-a-muddled-field-1 (last visited Feb 13, 2024).
- B. SHIVA RAO, THE FRAMING OF INDIA'S CONSTITUTION A STUDY (1968)", http://archive.org/details/in.ernet.dli.2015.275967 (last visited Feb 13, 2024).
- [1]18. M. P. Sharma And Others vs Satish Chandra, District ... on 15 March, 1954, https://indiankanoon.org/doc/1306519/ (last visited Feb 14, 2024).
- Wolf v. Colorado :: 338 U.S. 25 (1949) :: Justia US Supreme Court Center", https://supreme.justia.com/cases/federal/us/338/25/
- Prince Albert v Strange (1849) 47 ER 1302 | Student Law Notes - Online Case Studies, Legal Resources and Audio Summaries, https://www.studentlawnotes.com/prince-albert-v-strange-1849-47-er-1302 (last visited Feb 14, 2024).
- William Van Alstyne, *Closing the Circle of Constitutional Review from Griswold v. Connecticut to Roe v. Wade: An Outline of a Decision Merely Overruling Roe*, 1989 Duke Law Journal 1677 (1989).
- Michael Tilbury, *"Privacy": Common Law or Human Right?*, *in* Emerging Challenges in "Privacy" Law: Comparative Perspectives 157 (David Lindsay et al. eds., 2014), https://www.cambridge.org/core/books/emerging-challenges-in-"Privacy"-law/"Privacy"-common-law-or-human-right/3537CF826420DD4C1BA32188A0944625.
- Nicole Moreham, *Douglas and Others v Hello! Ltd. The Protection of "Privacy" in English Private Law*, 64 The Modern Law Review 767 (2001).
- Julia Carrie Wong (2019, March 18). The Cambridge Analytica scandal changed the world – but it didn't change Facebook, *The Guardian.* Retrieved from

www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook

- Edward J. (2018, May11) The Hacked & the Hacker-for-Hire: Lessons from the Yahoo "Data Breach"es (So Far).*The National Law Review*. Retrieved from www.natlawreview.com/article/hacked-hacker-hire-lessons-yahoo-data-breaches-so-far.
- Ode Holdings Inc. (2023, April 13), Top "Data Breach"es which effected millions of users. Retrieved from https://www.linkedin.com/pulse/top-data-breaches-which-effected-million-users-opendataeconomy
- Floridi, Luciano. 2015. "'The "Right to be forgotten"': A Philosophical View." Jahrbuch Für Recht Und Ethik / Annual Review of Law and Ethics 23:163–79.
- Travis, Alan, and Charles Arthur. 2014. "EU Court Backs '"Right to be forgotten': Google Must Amend Results on Request." *The Guardian*, May 13.
- Anon. n.d. "Art. 17 GDPR – Right to Erasure ('"Right to be forgotten"')." *General "Data Protection" Regulation (GDPR)*. Retrieved November 1, 2023 (https://gdpr-info.eu/art-17-gdpr/).
- William M. Beaney, The Constitutional Right to "Privacy", 1962 SUP.CT. REV. 212 (1962). See also Erwin Griswold, The Right to Be Let Alone, 55 NW. U. L. REV. 216 (1960)
- Leticia Bode & Meg Leta Jones, *Ready to Forget: American Attitudes toward the "Right to be forgotten"*, 33 The Information Society 76 (2017).
- Shaniqua Singleton, Balancing A "Right to be forgotten" with A Right to Freedom of Expression in the Wake of Google Spain v. Aepd, 44 Ga. J. INT'L & COMP. L. 165, 176 (2015).
- Rachit Garg, *R. Rajagopal and Ors. v. State of Tamil Nadu, 1994 SCC (6) 632 : Case Study*, iPleaders (Jan. 28, 2022), https://blog.ipleaders.in/r-rajagopal-and-ors-v-state-of-tamil-nadu-1994-scc-6-632-case-study/ (last visited Jun 9, 2023).
- Matt Andrews, Lant Pritchett & Michael Woolcock, *Looking like a State: The Seduction of Isomorphic Mimicry*, *in* Building State Capability: Evidence, Analysis, Action 0 (Matt Andrews, Lant Pritchett, & Michael Woolcock eds., 2017), https://doi.org/10.1093/acprof:oso/9780198747482.003.0003 (last visited Jun 12, 2023).

Case Laws:

- Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1
- Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295 (India)
- Lawrence v. Texas, 539 U.S. 558.(2003)
- People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301 (India)
- Roe vs. Wade, 410 U.S. 113 (1973).
- State v. Charulata Joshi, (1999) 4 SCC 65 (India) 21
- Gobind vs State Of Madhya Pradesh And Anr.
- R. M. Malkani vs State Of Maharashtra
- Shri Bodhisattwa Gautam vs Miss Subhra Chakraborty

- Meyer v Nebraska (1923)
- Griswold v. Connecticut
- Stanley v. Georgia
- Roe v. Wade
- Kelley v. Johnson, 425 U.S. 238 (1976)
- Ravin v. State, Justia Law (2024
- Moore v. City of East Cleveland
- Mosley v News Group Newspapers Ltd
- Katz v. United States, 389 U.S. 347, 359 (1967).

Legislation: National:

- The General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR)
- Privacy Act 1988 (Australia)
- Personal Data Bill 2011 (Brazil)
- Personal Data Act of Finland
- Federal Data Protection Act (Germany)
- Privacy Act of 1974 of USA

Indian:

- Information Technology Act 2000
- Bill - Personal Data Protection, 2019
- Indian Penal Code 1860
- Indian Evidence Act 187
- Digital Personal Data Protection Act 2023