CHAPTER 1: INTRODUCTION

1.1 Introduction

The never-ending aspect of the law is always intriguing, especially the field of technology law. We are constantly surrounded by technology. Technology Law is a new and growing field with a massive potential which will bring new opportunities and solutions on the table, like significantly reducing the cost and time of administration of justice, and the reduction in the justice gap.

The IAMAI-Kantar ICUBE[1] 2020 report estimates that the number of active internet users in India will increase to 900 million by 2025 from the present 622 million.[2] This increase is in direct correlation with the increase in smartphone usage in the country. According to the India Cellular & Electronics Association (ICEA) report, by 2022 there will be around 840 million smartphone users in India.[3]

India is yet to have its data protection law, a law which is at the utmost importance in the 21st century.[4] The Digital India initiative right now is in its prime, every day the government of India is launching a new e-Governance scheme for the public, new tech startups coming up every day and our reliance on technology is increasing day by day. However, all this is happening without a data protection law. Our shift to the digital world is at risk, our data is at risk without any law to protect our personal data, or to regulate the data sharing between different enterprises, and to prevent the risk of mass surveillance.

The topic of this Dissertation is **"Human Rights and Digital Rights in India: Impact on our Society and the Laws"**. The researcher chose this topic because the researcher is deeply passionate with the field of Technology Law and Policy.

In this dissertation, the researcher will focus the research on the importance of a good data protection law, its benefits and what could go wrong if case of its absence. The researcher will also discuss new and upcoming technologies like the emergence of Cryptocurrency and Blockchain and its impacts on our society, privacy and human rights and how it will impact the law making process of our country. The researcher will also share the analysis of the Draft Data Protection Bill[5] and mention different types of surveillance and its legal implications.

The importance of this topic arises due to the increasing number of internet users and e-Governance initiatives. When most people spend their time online, the most crimes also happen online. It is important for us to understand how to protect ourselves in the digital worlds and to know about the law which we have on our disposal.

1.2 Right to Privacy

Whether you are an activist, a celebrity, a politician, or just another ordinary person, privacy is for everyone.

On 24 August 2017, the Supreme Court of India in a historic judgement declared the right to privacy as a fundamental right protected under the Indian Constitution. In declaring that this right stems from the fundamental right to life and liberty.

The judgement was pronounced in response to a reference made in connection with the legal challenge to India's national identity project – Aadhaar – during which the Advocate General of India argued that the Indian Constitution does not include within it a fundamental right to privacy. His arguments were based on two cases decided by the Supreme Court – one, MP Sharma v. Satish Chandra decided by an eight judge bench in 1954 and the other, Kharak Singh v. State of Uttar Pradesh, by six judges in 1962. Both cases had held, in different circumstances, that the Constitution of India does not specifically protect the right to privacy.

Our privacy is in danger, and it is being constantly under attack by government agencies, big tech companies and non-state actors.

Government Agencies.

Governments across the globe indulge in state-sponsored surveillance to combat terrorism, prevent crimes, and to catch criminals. Unfortunately, surveillance is also used by governments for their political gains.

What type of protection is available to us against state-sponsored surveillance?

Over 150 national constitutions mention the right to privacy. In India, the Right to Privacy is a fundamental right. In addition to that, the Right to Privacy is enshrined in the Universal Declaration of Human Rights. There has been constant attempts to weaken our right to privacy, by attempting to control the use and the distribution of tools like End-to-End Encryption (E2EE).

Big Tech Companies.

In the last few years, we have seen a drastic change in the business model of companies. Big tech companies of our time like Amazon, Google, Facebook, Microsoft, etc. are solely depended on our data. They monetize our data, and sell it to advertisers. This type of business model allows free services and platforms like YouTube, Instagram or Google Search profitable.

> *“If you're not paying for the product, you are the product.”*

How true this statement is? We surely are not paying for the online services that we use, then how come we are the product?

We are not paying for free online services like Google Maps, Bing, YouTube, Facebook, Instagram, and Twitter with fiat currency, in fact, we are paying for them with our data. They use our data and our information to show us advertisements which we are most likely to click on. These platforms are designed to

be addictive, the more we spend our time on these social media platforms, the more ads they can show us.

Not only we have to ponder upon the data hogging business model of these companies, we also have to think about the ways they implement it. Social media is addictive by design.[6] And that design is serving the big tech companies.

Non-State Actors.

Non-state actors are individuals who indulge in illegal activities like cyber crimes to target others.

1.3 Research Methodology

The research conducted for this dissertation is “doctrinal” research. The sources of data used for this study are primary and secondary in nature.

1.3.1 Statement of Problem

The world is constantly changing, our reliance on technology is increasing day by day, the internet has become a basic necessity of life. As the internet has changed the workings of our life, it has also redefined what privacy is. Just like silence is only noticeable when noise is muted, privacy is only craved once it has been lost, and that exactly what is happening in China right now. Chinese authorities are using facial recognition to track its citizens, and in some cities, if Chinese citizens break a traffic law, they will get a ticket automatically and money will also be deducted from their account automatically. Will facial recognition technology in India is going to make governance easy and allow the law enforcement agencies to catch criminals before they commit any crime? Or will this technology be abused by the authorities? India is very different from China, one is a democratic country, the other is authoritarian. One has stronger civil liberties, the other has close to none. India, the largest democracy in the world and second-largest internet user base, has been trying to enact a national data protection law for quite some time now. At the same time, India is also exploring the horizons of facial recognition technology in few states.

In the most recent protests, the people of Hon Kong were fighting for democracy, which is something which we all take for granted. Being a democratic society is not enough for protecting civil liberties and defending privacy, which is a human right. Because even in the strongest of democracies, we risk losing our identity, our most intimate moments, our personal data. Invasive laws can be enacted anywhere in the world, even in the countries like the USA, Australia, and India. Australia enacted a law which bans cryptography, which is terrible for freedom of speech, India wants messaging apps to track the originator of the message, as a result, it will break encryption, again a terrible move for freedom of speech.

Though, more people live outside of China and hence immune to their invasive tracking, unfortunately they are not immune from the Big Tech companies. We are using payments apps with cash back options to purchase items from Amazon, which does not even allow you to delete your purchase history. We are sharing our personal photos with our friends on social media. We use Google every day to find answers to our most

embarrassing questions. What we do not realise is that in this process we are allowing these companies to collect a large amount of data about us, and how we use their services. This is not a big issue by itself, maybe for some people it is and that is why they choose to use privacy-friendly alternatives, but for the majority it is not, or the majority believe it is not a big issue. To be fair, these companies collect data about us to show us more relevant ads. The problem begins when ad tech becomes surveillance tech. When government agencies start asking (or forcing) these companies to share the data they collect with the government as well. The problem begins when we realise that these companies can go to any extent to earn more profits. Facebook knows that their products can be harmful to certain sections of the society, for example Instagram is likely to affect the mental healths of teenage girls, yet they are not wiling to address this issue because by doing so, they will lose profits. It is important that we as a society come up with laws which are designed to protect our privacy. Privacy is a sensitive matter, under no circumstances it should be exposed to third parties without the consent of the actual owner of that personal data.

We all care about privacy, you will never give out our password to anyone or share your secrets with any strangers, then why let these companies know what you are thinking about. We all care about privacy, we call want freedom, we all look up to democracy. The true price of convenience is freedom, we are feeding nation states and companies a huge amount of information. This is fine as long it is fine, but the moment this crosses the line, freedom is no more. In order to defend our freedom, and protect our privacy, we need to first claim our digital rights first.

1.3.2 Review of the Literature

To achieve the aims and objectives of this research, the researcher has followed research articles, reports and books, some of which are mentioned hereinafter.

Permanent Record by Edward Snowden (September 2019), Published by Macmillan Publishers Ltd.

Permanent Record is a 2019 autobiography by Edward Snowden, whose revelations sparked a global debate about surveillance. The book describes Snowden's childhood as well as his tenure at the Central Intelligence Agency and National Security Agency and his motivations for the leaking of highly classified information in 2013 that revealed global surveillance programs. Snowden also discusses his views on authoritarianism, democracy, and privacy.

The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data by Kevin Mitnick (February 2017), Published by Little, Brown and Company.

In this explosive yet practical book, Kevin Mitnick uses true-life stories to show exactly what is happening without your knowledge, teaching you “the art of invisibility” – online and real-world tactics to protect you and your family, using easy step-by-step instructions. Reading this book, the author explains everything from password protection and smart Wi-Fi usage to advanced techniques designed to maximize your anonymity. Kevin Mitnick knows exactly how vulnerabilities can be exploited and just what to do to prevent that from happening.

The Age of Surveillance Capitalism by Shoshana Zuboff (2019) Published by Profile Books.

The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power is a 2019 non-fiction book by Shoshana Zuboff which looks at the development of digital companies like Google and Amazon, and suggests that their business models represent a new form of capitalist accumulation that she calls “surveillance capitalism”

While industrial capitalism exploited and controlled nature with devastating consequences, surveillance capitalism exploits and controls human nature with a totalitarian order as the endpoint of the development.

Digital Disconnect How Capitalism Is Turning the Internet Against Democracy by Robert W. McChesney (March 5, 2013) Published by The New Press.

In this book, the author argues that the sharp decline in the enforcement of antitrust violations, the increase in patents on digital technology and proprietary systems and massive indirect subsidies and other policies have made the internet a place of numbing commercialism. A handful of monopolies now dominate the political economy, from Google, which garners a 97 percent share of the mobile search market, to Microsoft, whose operating system is used by over 90 percent of the world's computers. Capitalism's colonization of the Internet has spurred the collapse of credible journalism and made the Internet an unparalleled apparatus for government and corporate surveillance and a disturbingly antidemocratic force.

In Digital Disconnect, Robert McChesney offers a groundbreaking critique of the Internet, urging us to reclaim the democratizing potential of the digital revolution while we still can.

The Great Tech Game: Shaping Geopolitics and the Destiny of Nations by Anirudh Suri (May 2021) Published by Harper Collins India.

In The Great Tech Game, the author provides a coherent framework outlining the key drivers that will determine the ability of a nation to succeed in this technology-dominant era. He lays out a roadmap for how any country must develop its own strategic plan for success. Leaders must inculcate a new set of capabilities to understand and take advantage of these trends, and create enabling environments for their nations to not be left behind. A particularly challenging aspect will be the ability of countries to define and manage the roles of state and non-state actors in a global race for technological leadership and success. The book goes on to evaluate whether digital colonialism is an inevitable reality, or whether new frameworks will emerge to govern relationships between technology-rich and technology-poor nations.

Game On: Exploring the Impact of Technologies on Young Men’s Mental Health and Wellbeing.

By Jane M. Burns, Tracey A. Davenport, Helen Christensen, Georgina M. Luscombe, John A. Mendoza, Amanda Bresnan, Michelle E. Blanchard, Ian B. Hickie.

This report focuses specifically on young men aged 16 to 25.[7] Technologies have changed the way young people communicate, connect and engage with each other and with society. Young people use the internet to find and share information, to support their friends, and to reach out via social networks to others who might be experiencing similar challenges. With the introduction of smartphones, information and services provided online or via mobile applications can be accessed privately and at any time. This can be empowering for

individuals who are marginalised or geographically or socially isolated. For the first time in history, it is possible to reduce the disparities in access to health care as a result of isolation, stigma, or cost.

Surveillance and Censorship: The Impact of Technologies on Human Rights.

By Ben Wagner, Joanna Bronowicka, Cathleen Berger.

This paper is about surveillance and censorship and how it impacts our human rights. As human lives transition online, so do human rights. The main challenge for the European Union and other actors is to transition all human rights to the digital sphere. This report argues that the human rights-based approach can be helpful in focusing discussions about security on individuals rather than states. It provides an overview of countries and companies that pose risks to human rights in the digital sphere. It lists the most relevant international laws and standards, technical standards, business guidelines, Internet principles and policy initiatives that have been crucial in transitioning the human rights regime to the digital sphere.

The article also analyses the impact of recent EU actions related to Internet and human rights issues. It concludes that different elements of EU strategic policy on human rights and digital policy need to be better integrated and coordinated to ensure that technologies have a positive impact on human rights. The report concludes that the EU should promote digital rights in national legislation of the third countries, but also in its own digital strategies.[8]

The Right of Privacy, Harvard Law Review, 1989.

By Jed Rubenfeld

This article is about the constitutional right to privacy, a right that many believe has little to do with privacy and nothing to do with the Constitution. By all accounts, however, the right to privacy has everything to do with delineating the legitimate limits of governmental power.

The right to privacy, like the natural law and substantive due process doctrines for which it is a late-blooming substitute, supposes that the very order of things in a free society may on certain occasions render intolerable a law that violates no express constitutional guarantee. For three decades, the right to privacy has served as a constitutional limit on governmental power. Despite the importance of this doctrine and the attention that it has received, there is little agreement on the most basic questions of its scope and derivation.[9]

Data Protection Regulations in India and The Significance of Consent Framework.

By Bharath Chandran P S

This article talks about the data protection regulations in India and the significance of consent framework present in India. Every activity we do in the digital sphere generates data, with or without our consent. Similarly, the generated data may be personal or non-personal data. Even with the huge amount of data being collected and processed there have been no specialized laws that focus on the protection of the data.

The main question that arises in this regard is the nature of the data collected, the purpose for its collection, the duration for which the data is stored, which entities are provided access to the data, what is done with the data after the specified use and what are the measures in case of breach of these collected data.[10]

1.3.3 Objective of the Study

The researcher through this research aims to achieve the following objectives:

1. To understand the meaning of the Right to Privacy.
2. To understand the historical evolution of the Right to Privacy laws in India.
3. To understand how Big Tech companies monetise our personal data for their profit.
4. To understand how fake news and misinformation can impact our democracies and elections.
5. To understand how Right to Privacy is a Human Right.
6. To understand the available legal options in the world to protect an individual's Right to Privacy.
7. To understand the available legal options in India to protect an individual's Right to Privacy.

1.3.4 Research Question

This research aims to answer the following questions:

Q 1. How emerging technologies are impacting our society and the growth?

Q 2. How emerging technologies are impacting our legal system?

Q 3. What is Right to Privacy?

Q 4. How is Right to Privacy recognised in India?

Q 5. What is the importance of Right to Privacy?

Q 6. How to strengthen the Right to Privacy in the digital world?

1.3.5 Hypothesis

With proper education and learning, along with the support of right legislation and a strong data protection mechanism, it is possible to control our privacy and prevent a dystopian future.

1.3.6 Scope and Limitations

The scope of this research is to study the impact of emerging technologies on us, and how it is influencing the growth of the laws of our land. This research aims at spreading awareness about the Right to Privacy and its violations as a Human Rights issue.

The researcher will look into the legal frameworks in place in India and as well as in other countries. This is a study with critical analysis of legislative framework, judicial decisions and policy work. The study involves analyses of primary data in the form of legislation, judicial decisions, and government policies. It would also involve detailed study of secondary sources such as various scholarly articles, case studies, books on the subject and foreign laws.

The research conducted for this dissertation is “doctrinal” research. The sources of data used for this study are primary and secondary in nature. A host of leading textbooks of Indian and International authors on law relating to human rights, right to privacy, freedom of speech, etc. have been referred to.

Articles and essays from leading newspapers like The Hindu, and The Indian Express, various books, and journals, along with online articles published by various reputed organisations have been used in this research by the researcher.

Apart from all these secondary resources, many landmark cases and government documents and reports are also used in this research by the researcher.

1.3.7 Chapterisation

Chapter 1: Introduction

In this chapter, the researcher gives an introduction to this dissertation, along with a brief introduction to what Right to Privacy is, and why it is important for a healthy democracy, and for our freedom of speech.

Chapter 2: Human Rights and Right to Privacy.

In this chapter, the researcher explained the concept of right to privacy in India and the evolution of the privacy law in India. The researcher relies upon various judgements to explain India's stand on right to privacy. The researcher in this chapter also explains why the right to privacy is a human right, and why one should defend its digital rights.

Chapter 3: Right to Privacy in Cyberspace.

This chapter is all about social media and Big Tech companies. In this chapter, the researcher talks about the impacts of social media on our mental health, democracy, elections, and most importantly on our right to privacy and human rights.

The researcher also emphasis the need to be aware of the data collection and surveillance done by private companies for their profit, and give examples on how one can protect themselves.

At the end of this chapter, the researcher discusses the need to combat misinformation and fake news, and share strategies on how a person can detect fake news.

Chapter 4: Digital Rights Around the World.

In this chapter, the researcher mentioned various laws related to right to privacy and technology around the world and in India. In this chapter, the researcher has mainly covered the following countries; USA, Germany, United Kingdom, Spain, and India. The researcher has compared these laws and explained how governments in these countries intercept our personal communications.

Chapter 5: Conclusion and Suggestions.

The concluding chapter provides an overall analysis of the observations made in the dissertation by the researcher and their understanding of the issues surrounding the impact of emerging technologies on our society and the laws, the statutory framework and the extent of its effectiveness in the Indian society. This Chapter concludes the study by coming up with logical answers to the questions set in Chapter One as supported by the doctrinal evidence collected and analysed in the preceding chapters. This chapter culminates with numerous suggestions by the researcher.

Endnotes:

1"Internet usage in India to grow exponentially by 2025", Ministry of External Affairs, Government of India. https://indbiz.gov.in/internet-usage-in-india-to-grow-exponentially-by-2025/ Last Accessed on 5 April 2022.

2"India to have 900 million active internet users by 2025, says report", The Economic Times. https://economictimes.indiatimes.com/tech/technology/india-to-have-900-million-active-internet-users-by-2025-says-report/articleshow/83200683.cms Last Accessed on 5 April 2022.

3"ICEA report: 83 crore smartphone users by 2022", The Indian Express. https://indianexpress.com/article/technology/tech-news-technology/icea-report-83-crore-smartphone-users-by-2022-6499952/ Last Accessed on 5 April 2022.

4PRS India, "The Personal Data Protection Bill, 2019", PRS Legislative Research. https://prsindia.org/billtrack/the-personal-data-protection-bill-2019 Last Accessed on 5 April 2022.

5"The Personal Data Protection Bill, 2018", Ministry of electronics and Information Technology, Government of India.
https://www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf Last Accessed on 5 April 2022.

6'The Wall Street Journal', “How TikTok's Algorithm Figures You Out” YouTube. https://www.youtube.com/watch?v=nfczi2cI6Cs Last Accessed on 8 May 2022.

7Burns, J. (2013). Game on: Exploring the impact of technologies on young men's mental health and wellbeing. Last Accessed on 6 May 2022.

8Ben WAGNER, J., Internet, T. & Human Rights, E., 2015. Surveillance and Censorship: The Impact of Technologies on Human Rights, EPRS: European Parliamentary Research Service. Retrieved from https://policycommons.net/artifacts/1336405/surveillance-and-censorship/1943517/ on 06 May 2022. CID: 20.500.12592/2g5tt0. Last Accessed 6 May 2022.

9Rubenfeld, Jed. “The Right of Privacy.” Harvard Law Review, vol. 102, no. 4, 1989, pp. 737–807, https://doi.org/10.2307/1341305. Accessed 6 May 2022.

10Bharath Chandran P S, Data Protection Regulations in India and The Significance of Consent Framework, 3 (5) IJLSI Page 111 - 127 (2021), DOI: https://doij.org/10.10000/IJLSI.111060 Last Accessed on 7 May 2022.

Revision #3
Created 6 November 2022 12:53:19 by ponytail
Updated 6 November 2022 13:12:31 by ponytail