AUTHENTICATION OF BIOMETRICS IN BUSINESS TRANSACTIONS AND WORKPLACE IN INDIA VIS -A – VIS DATA PRIVACY – A CRTICAL STUDY .

Dissertation submitted to National Law University and Judicial Academy, Assam

In partial fulfilment for award of degree of

Master of Laws (LLM)

ONE YEAR LLM DEGREE PROGRAMME (2020-2021) BATCH

Submitted by

Trishna Devi

UID- SF0220031

LLM 2nd Semester, 2020-2021 Batch

Supervised by

Dr Daisy Changmai,

Guest Faculty of Law

National Law University and Judicial Academy, Assam

July 2020

SUPERVISOR CERTIFICATE

This is to certify that Ms. TRISHNA DEVI is pursuing Master of Laws (LL.M) from National Law University and Judicial Academy, Assam has completed her dissertation "AUTHENTICATION OF BIOMETRICS IN BUSINESS TRANSACTIONS AND WORKPLACE IN INDIA VIS -A – VIS DATA PRIVACY – A CRTICAL STUDY " under my supervision for the partial award of the degree of Master of Laws (LLM) ONE YEAR LLM DEGREE PROGRAMME (2020-2021) Batch. The research work is found to be original and suitable for submission.

Date : 28/07/2021

Assam

DR.DAISY CHANGMAI

GUEST FACULTY OF LAW

NATIONAL LAW UNIVERSITY AND JUDICIAL ACADEMY, ASSAM

DECLARATION

I, TRISHNA DEVI , pursuing Master of Laws (LL.M) 2020 -2021 batch from National Law University and Judicial Academy, Assam, do hereby declare that the dissertation titled "AUTHENTICATION OF BIOMETRICS IN BUSINESS TRANSACTIONS AND WORKPLACE IN INDIA VIS -A – VIS DATA PRIVACY – A CRTICAL STUDY." submitted by me for the award of the degree of MASTER OF LAWS/ ONE YEAR LL.M. DEGREE PROGRAMME of National Law University and Judicial Academy, Assam is a bonafide work and has not been submitted, either in part or full anywhere else for any purpose, academic or otherwise.

Date: 28.07.2021

TRISHNA DEVI

UID- SF0220031

LLM 2nd Semester, 2020-2021 Batch

TABLE OF CONTENTS

ACKNOWLEDGEMENT

I acknowledge with pleasure, National Law University and Judicial Academy, Assam for its unparallel infrastructural support and its rich academic resources. I am highly elated to work on the topic of "AUTHENTICATION OF BIOMETRICS IN BUSINESS TRANSACTIONS AND WORKPLACE IN INDIA VIS -A – VIS DATA PRIVACY – A CRTICAL STUDY." under the able guidance of my supervisor, Dr Daisy Changmai, Guest Faculty of Law, National Law University and Judicial Academy, Assam.

First of all, I would like to express the deepest gratitude towards mu guide and supervisor Dr Daisy Changmai, Guest Faculty of Law who has been of immense help and guided me throughout the research. Throughout the writing of this research paper, I have received a great deal of support and assistance from her , without the guidance of her this paper would not have been possible as she provided me with the right direction regarding this research.

Second of all I would like to thank Prof (Dr) V. K. Ahuja, Vice Chancellor of National Law University and Judicial Academy, Assam for providing me an opportunity to embark on this research paper and also for sharing his vast knowledge.

Thirdly , I am grateful to Dr. Indranoshee Das, ACS, Registrar, National Law University and Judicial Academy, Assam and Dr. Nandarani Choudhury, Assistant Registrar, National Law University and Judicial Academy, Assam for their priceless and untiring support.

Fourthly, I would like to express my sincere thanks and gratitude to Dr. Kankana Baishya, Assistant Librarian, National Law University and Judicial Academy, Assam and the library staff members of National Law University and Judicial Academy, Assam who rendered there help during the period of my research

paper . I want to thank you for your excellent cooperation and for all of the opportunities I was given to conduct my research

I am also greatly indebted to the various writers, jurists and all other authors from whose writings and literary works I have taken help to complete this research paper.

Finally, I humbly submit before the Almighty whose grace has made everything possible.

TRISHNA DEVI

UID- SF0220031

LLM 2nd Semester, 2020-2021 Batch

TABLE OF CASES

TABLE OF STATUTES

1966	The International Covenant on Civil and Political Rights (ICCPR), 1966
2000	Information Technology Act
2008	Illinois Biometric Information Privacy Act
2011	The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (Privacy Rules)
2016	Aadhar (Enrolment and Update) Regulations , 2016'
2017	Texas Capture or Use of Biometric Identifier Act (CUBI)
2017	Washington House Bill 1493
2018	General Data Protection Regulation (GDPR), 2018
2018	United Nations Compendium of Recommended Practices for the Responsible Use and Sharing of Biometrics in Counter-Terrorism, 2018
2019	Personal Data Protection Bill, 2019
2020	California Consumer Privacy Act (CCPA)

TABLE OF ABBREVIATION

Sl No	Abbreviation	Full Form
1)	AI	Artificial Intelligence
2)	Anr	Another
3)	API	Application Programming Interface
4)	Art	Article
5)	BAS	Biometric Attendance System
6)	BIPA	Illinois Biometric Information Privacy Act
7)	CCPA	California Consumer Privacy Act
8)	CIA	Central Intelligence Agency
9)	CTED	Counter-Terrorism Committee Executive
10)	CUBI	Texas Capture or Use of Biometric Information
11)	DNA	Deoxyribonucleic acid
12)	DPA	Data Protection Authorities
13)	Dr	Doctor
14)	EAB	European Association for Biometrics
15)	E-governance	Electronic Governance
16)	EU	European Union
17)	F.B.I	Federal Bureau of Investigation
18)	FERET	Face Recognition Technology Evaluation
19)	FIDO	Fast Identity Online
20)	GDPR	General Data Protection Regulation
21)	IAFIS	Integrated Automated Fingerprint Identification System
22)	ICCPR	The International Covenant on Civil and Political Rights
23)	ID	Identity Document
24)	ISO	International Organisation for Standardization
25)	IT	Information Technology
26)	KYC	Know Your Customer
27)	MRTD	Minimum Resolvable Temperature Difference
28)	NIST	National Institute of Standards and Technology

29)	NSA	National Security Agency
30)	Ors	Others
31)	Retd	Retired
32)	SCC	Supreme Court Cases
33)	SOP	Standard Operating Procedure
34)	UIDAI	Unique Identification Authority of India
35)	UK	United Kingdom
36)	UN	United Nations
37)	UNHRC	United Nations Human Rights Committee/ Council
38)	USA	United States of America
39)	v	versus
40)	WP	Working Party

CHAPTER 1

INTRODUCTION

1.1 Introduction

The advent of the 21st century has seen rapid development in technology in all sectors. Organisations and businesses have stated to change from manual systems and processes to automated and technological processes. One of the foremost changes that been forefront in the last decade in the world is the innovation and development in automated biometric systems. Researchers and technicians around the started to develop systems that are capable of identifying people automatically through facial recognition, voice, fingerprints, etc. Law enforcement agencies have specially has long used fingerprints as forensic evidence. The development of biometric systems allowed law agencies to use biometric data to store fingerprints and facial image of suspects in their database and cross check it later for forensic and criminal identification and profiling. The FBI as the early 1990's was using biometric system for criminal identification. Later the governments of countries started using biometric data by incorporating it in citizen IDs or social security ID's and used them for welfare schemes, access to offices, availing of certain government services, civilian identification and many other things. Later businesses began to be interested in biometrics and many industries began the adoption of biometrics for commercial purposes and others. By the latter half of the last decade use of biometrics to identify and verify became extremely commonplace. Technological advancements and developments showed the innovation of new and advanced biometric systems that went from being large bulky machines to small handheld fingerprint scanner to availability of authentication facilities in mobile phones, laptops and many other small devices. Such developments encouraged the use of biometrics in businesses, workplaces, at home and everywhere. People were either buying devices that had in built biometric

system or linking their devices to biometric devices as it was extremely convenient to use, for unlike in other devices, these devices allowed a person to perform some tasks by the simple action of authenticating their biometrics and there was no need to remember PINs or lengthy passwords. Also, it had the added security of being unable to be stolen being biological characteristics. Companies and organisations had started to use biometrics in their offices for authentication cases.

In India, Aadhar Act heralded the era of biometric identity card and number. After that it became very common place in India to use biometric systems. Before that, biometrics were generally used for military, law enforcement, research labs and departments, places requiring specific access and others. In businesses and workplaces biometric data authentication had mainly been used before for purposes like accessing confidential areas or spaces, to provide access for confidential files, to verify the identity of the person and others. However, after 2011, there has been use of biometric data authentication for all things like recording attendance, accessing rooms, verifying identities, doing commercial transactions, opening accounts and many other things. Slowly , biometric authentication has become a norm for people. "However, Biometric Data being our most personal and sensitive data is not free from the flaws in the system and is vulnerable to many issues such as data privacy and security and authentication issues. In India, there is still no exhaustive and comprehensive laws on the usage of biometric data that reflects international standard. This paper aims to study the introduction of Biometric Data, Authentication in India regarding workplaces and business transactions and the data privacy laws that govern the use and authentication of biometrics is workplaces and business transactions. This paper will delve into prevalent legal framework that governs such practices and study and analyse how the current rules apply to the present scenario."

1.2 Statement of the problem

Biometrics are largely used in today's world and with the increasing use of biometrics it has become commonplace for people from all walks of life to use biometrics in this everyday life. It is estimated that Indian Biometric market will grow by billions of dollars. Also, nowadays from workplaces to business transactions to e-commerce transactions to home devices all see the heavy usage of biometric data. Biometric data has been considered sensitive personal data and therefore there is need to regulate usage of such data. There is a need to protect the privacy of people and make sure that such data is confidential and secure. Herein, comes the role of the law, especially data privacy and data protection laws. With the increased use of biometrics in office spaces and for purposes of business transactions, there is a need to study the data privacy laws that apply to such a matter and ensure that such legislation is sufficient.

1.3 Aim

The aim of this paper is to study the concept of biometrics and their authentication used by people in business transactions and workplaces. The paper's main focus is on the study of the data privacy and protection rules surrounding biometric data in India . The paper looks at a couple of international legislations regarding biometrics. The paper comprehensively tries to study all the laws relating to biometric data in context of business and workplace in India and at the same time tries to test if the present laws are effective and comprehensive .

1.4 Objectives

The objectives of this paper are as follows:

1. To understand the concept of biometrics

2. To understand what are biometric characteristics and biometric identification and authentication

3. To understand the usage of biometrics in Business transactions and workplaces

4. To analyse the legal framework of biometric data in India in context of data privacy.

5. To study whether the legal mechanism ensures comprehensive data privacy regarding biometrics in India.

6. To study whether the present legal framework in India is effective and comprehensive

7. To make suggestions to streamline the existing regulatory framework

1.5 Scope and limitation

The scope of the study is to understand about the authentication, identification and usage of biometric data in today's workplaces and businesses, commercial transactions and business transactions. The research is limited to biometric data and the data privacy laws that is for the time being in force in India. Hence, it studies the concept of biometrics and usage of biometric data in business transaction and workplace. The paper studies all prevalent laws for data privacy related to biometric data and tries to analyse with the usage of such data in present day's workplaces and business transactions. The study doesn't go into other data privacy provisions not related to Biometric Data and there is slight mention of the Aadhar Law as the law although dealing with biometrics, is mostly controlled and operated by the government.

Although, the researcher has made a lot of efforts to gather all the available materials and data, however it was quite difficult to do so without access to physical library and the researcher is still not content. A lot of issues have been faced by the researcher due to the pandemic. The researcher as has said before was unable to access the library to get authentic books on the subjects. The researcher was also unable to get empirical data due to the ongoing pandemic. Secondly, while there have

been laws, lot of articles and even books on data privacy, most books and articles on biometric data in Indian context is all related to the Aadhar Act. India does not have a separate biometric law or even Act and further even very little study has been done on usage of biometrics in workplaces and data privacy in a systemised manner. Thirdly, even though the research is an individual endeavour, the importance of consultation of experts and other related persons to the topic is invaluable. However, due to the pandemic the researcher was unable to do so. Hence, the study and the research are extremely limited to the available secondary sources of research available to the researcher and the area is limited only to India.

1.6 Literature review

1.6.1 A.K. Jain, P Flynn and A. A. Ross (eds) Handbook Of Biometrics (2nd ed Springer 2007)

The book provides the very basic introduction to the world of biometrics and biometric data and is one of the oldest literatures on the topic. The book begins with an introduction to the biometrics and what is biometric data. This book is a collection of research articles written by prominent writers and researchers who has written about the fundamentals of the biometrics and also the new and advanced technologies of biometrics. The editors and the researchers have prepared the book as a handbook for people to learn about biometric data. The second chapter introduces the concept of fingerprint recognition and tells on the history of fingerprint recognition and also expands on the issues with fingerprint recognition. In the same vein the next few chapters of the book are dedicated to face recognition, iris recognition, hand geometry recognition and other biometric characteristics. The book and the articles discuss in details the working and classification of the biometric characteristics. The article in the book by Woodland, John D., Jr on the Law and Use of Biometrics deals with the legal framework and issues relating to biometric data, however most of the article only discusses law or legal framework of USA. The book also discusses how biometrics has been

used in the commercial sector, its challenges, history, effects and laws in the chapter Biometrics in the Commercial Sector by Prabhakar, Salil and others. There are also chapters that expand on Biometric Standards and biometrics databases. The Biometric Standards chapter provide for the role of Standards and the importance of biometric standards. The Biometric Databases talks about biometric recognition system and puts forward details on databases and what is biometric database and how they should operate.

1.6.2 Samir Nanavati, Michael Thieme and Raj Nanavati, Biometrics Identity Verification in a Networked World, Wiley Computer Publishing, 2002

The authors here talk about biometric technology, its fundamentals and details on biometric data. The first part begins with the fundamentals of biometrics. The first chapter emulates on the advantage of biometrics, with the second chapter providing for key terms and processes. The first part also talks about the technical details about the biometric systems especially on what is considered as accuracy. The second part of the book talks about the leading biometric technologies used in today's world. It provides detailed explanations the types of biometrics data such as finger-scan, facial-scan, iris scan, voice scan and other attributes. The third part of the book talks about biometric applications and markets. The author also highlights the issues regarding privacy in biometric data. The book talks about assessing the privacy risks that using biometric data provides and provides for new technological systems and standards that are privacy friendly and sympathetic and would more or less ensure confidentiality and security of data. The article also outlines the various biometric standards and discusses in the detail the various biometric standards given by different organisations

1.6.3. Els J. Kindt, Privacy and Data Protection Issues of Biometric Applications ,2013, A Comparative Legal Analysis, Law, Governance and Technology Series, Volume 12, Springer, 2013

It is one of the leading books on biometric data and data protection issues. The author has focused on European Laws and compared it with other laws. The author here critically analyses the Directive EC/95/46. This book discusses all critical privacy and data protection aspects of biometric systems from a legal perspective. It contains a systematic and complete analysis of the many issues raised by these systems based on examples worldwide and provides several recommendations for a transnational regulatory framework. An appropriate legal framework is in most countries not yet in place.

Biometric systems use facial images, fingerprints, iris and/or voice in an automated way to identify or to verify (identity) claims of persons. The treatise which has an interdisciplinary approach starts with explaining the functioning of biometric systems in general terms for non-specialists. It continues with a description of the legal nature of biometric data and makes a comparison with DNA and biological material and the regulation thereof. After describing the risks, the work further reviews the opinions of data protection authorities in relation to biometric systems and current and future (EU) law. A detailed legal comparative analysis is made of the situation in Belgium, France and the Netherlands.

The author concludes with an evaluation of the proportionality principle and the application of data protection law to biometric data processing operations, mainly in the private sector. Pleading for more safeguards in legislation, the author makes several suggestions for a regulatory framework aiming at reducing the risks of biometric systems. They include limitations to the collection and storage of biometric data as well as technical measures, which could influence the proportionality of the processing.

The text is supported by several figures and tables providing a summary of particular points of the discussion. The book also uses the 2012 biometric vocabulary adopted by ISO and contains an extensive bibliography and literature sources. The article criticises the Government for supporting the industries by speeding up the environment clearance for development projects. The draft notification clearly tries to weaken the already inadequate procedure for environment clearance. The author here lays down how this qualitative process is turning into quantitative nature. The no of projects which are grated clearance has been increasing with time and the number of the rejected project are falling lower than a per cent. The author here states the government's inclination towards development over environment is very clear from the draft notification.

1.6.4 AMBA KAK, ed., REGULATING BIOMETRICS: GLOBAL APPROACHES AND URGENT QUESTIONS,52-62 (Al Now Institute, 2020)

The theme of this compendium is the global standards of regulating Biometric Data. The author emphasises on the public scrutiny and interest in regulating biometric technologies that grown across the globe. The compendium begins with an introduction and a summary chapter that identifies key themes from existing legal approaches, and poses open questions for the future. These questions highlight the critical research needed to inform ongoing national policy and advocacy efforts to regulate biometric recognition technologies.

Regulating Biometrics: Global Approaches and Urgent Questions presents eight case studies from academics, advocates, and policy experts offering a variety of perspectives and national contexts. These expert contributors illuminate existing attempts to regulate biometric systems, and reflect on the promise, and the limits, of the law. The author further analyses the presence of regulatory framework around the globe for favour of data safety and data privacy provisions Therefore, the policy makers should nevertheless

question whether these regulations do all that can be done to produce a safer workplace or business transaction and data privacy.

1.6.5 Latha R Nair, 'Data Protection Efforts in India: Blind Leading the Blind' (2008) 4 Indian J L & Tech 19

The article here establishes the necessity for effective data protection in India and goes on to define the undeveloped measures taken in the country till date in the domain of data protection. While highlighting the insufficiency of such procedures and the vagueness in proposed amendments, the author seeks motivation from European Union law in proposing a broad framework for data protection law in India.

The first chapter begins with the necessity of data protection and what are the various reasons for safety of data and consequences of not protecting data. The second chapter describes in detail the existing legal framework in India. It analyses the Contract Law and the possibility of data protection through contract. The author then outlines in detail the Information Technology Act, 2000 and discusses its provisions in relation to data protection. The third chapter goes on to discuss as how over the time there were proposed amendments and other bodies were established and goes on to discuss these efforts in detail. The author concludes the article by saying that the efforts were not enough and the proposed amendments are still outdated and the bodies are not able to function properly and ensure protection of data.

1.6.6 Dhira R Duraiswami, 'Privacy and Data Protection in India' (2017) 6 Journal of Law & Cyber Warfare 166, 2017

The author examines the scope of privacy and data protection in India. The article provides an overview on the current privacy and data protection laws in India, the enforcement and liability of these laws and any pending regulations and trends to protect the privacy and enhance data protection. The first part of the article gives an overview of the

regulatory framework and talks about the concept of personal data. It analyses the different laws related to it like the IT Act 2000 and other rules and regulations. It also discusses cases related to data privacy and protection. The article also discusses the recent trends and industry initiatives like the National Association of Services and Software Companies and others. The article concludes with the opinion that there is lack of comprehensive legislation and there is need to update privacy and protection rules.

1.6.7 Singh, Atul. "DATA PROTECTION: INDIA IN THE INFORMATION AGE." (2017) vol. 59, no. 1, *Journal of the Indian Law Institute*, 78

This article is a paper on the data protection in India in the information age. The paper deals with personal data and the laws providing protection of such personal data in India. The author emphasises that in today's world information is power and talks about international laws also. In the article, the author analyses on the data security provisions on India. The article puts emphasis on the OCED guidelines. The articles deal with several significant aspects of statutory personal data protection laws, where the author puts emphasis on other aspects of data protection that has been addressed by electronic data storage laws. The author puts emphasis on an individual's right regarding data and data protection laws. The article analyses the Information Technology Act, 200 in relation to the protection of electronic data. The author has analysed the right to information in regards to access of personal data by the data subject. The author also talks about biometric information and core biometric information used to make ID and data protection laws related to it

1.6.8 Nguyen, Fiona Q. "The Standard for Biometric Data Protection." 2018, Vol 7 no 1. Journal of Law & Cyber Warfare, 61–84.

In this article the author tires to find the ideal standard for biometric data protection. The article first lays down the concept of biometrics, biometric data, characteristics of biometric data and others. The author tries to study and analyse as to why the characteristics of biometric data need protection . The article lays down why data protection is necessary regarding biometric data . It provides that for the enjoyment of right to privacy and to remain incognito there is need to protect biometric data and goes on to detail the intrusiveness done by government or others, data breach and profiling and leaking of data. The author then proceeds to analyse the current legislations in the United States, the article also outlines why a national biometric standard and need for a federal biometric law. The article then explains as to why a national biometric standard is necessary and how biometric data is used. The author also outlines and analyses other legislations around the world. It outlines cases where profiling happened and there was misuse of biometric data. The author concludes the article with saying that implementing GDPR approach in the USA will give more ability to control their biometric data.

1.6.9 NAYAR, PRAMOD K. "'I Sing the Body Biometric': Surveillance and Biological Citizenship." 2012, vol. 47, no. 32 Economic and Political Weekly, 17–22.

This article came about as a result of the Aadhar Act 2016. The author here has analysed the concept of biological citizenship through the application of biometrics that has been used in Aadhar to ensure a unique identity number to every citizen. The article analyses the Aadhar Act and the concept of identity, identification and biometrics. The author also talks about state surveillance that is being used to keep an eye on the

masses and how the government monitors every move of the citizens. The article explains and analyses issues such as rematerialized bodies, software programming , body privacy, wish to be incognito and remain anonymous, biometric borders, mobile borders, and others arising when we talk about biological citizenship. The article talks about mass surveillance and profiling. And at the last the article talks about biological citizenship, study its particulars and analyses its pros and cons and the danger of such citizenship.

1.7 Research question

1. Whether there is effective present legal mechanism in India regarding authentication and use of biometrics in business and workplaces?

2. What are the data privacy laws in concern with biometric data?

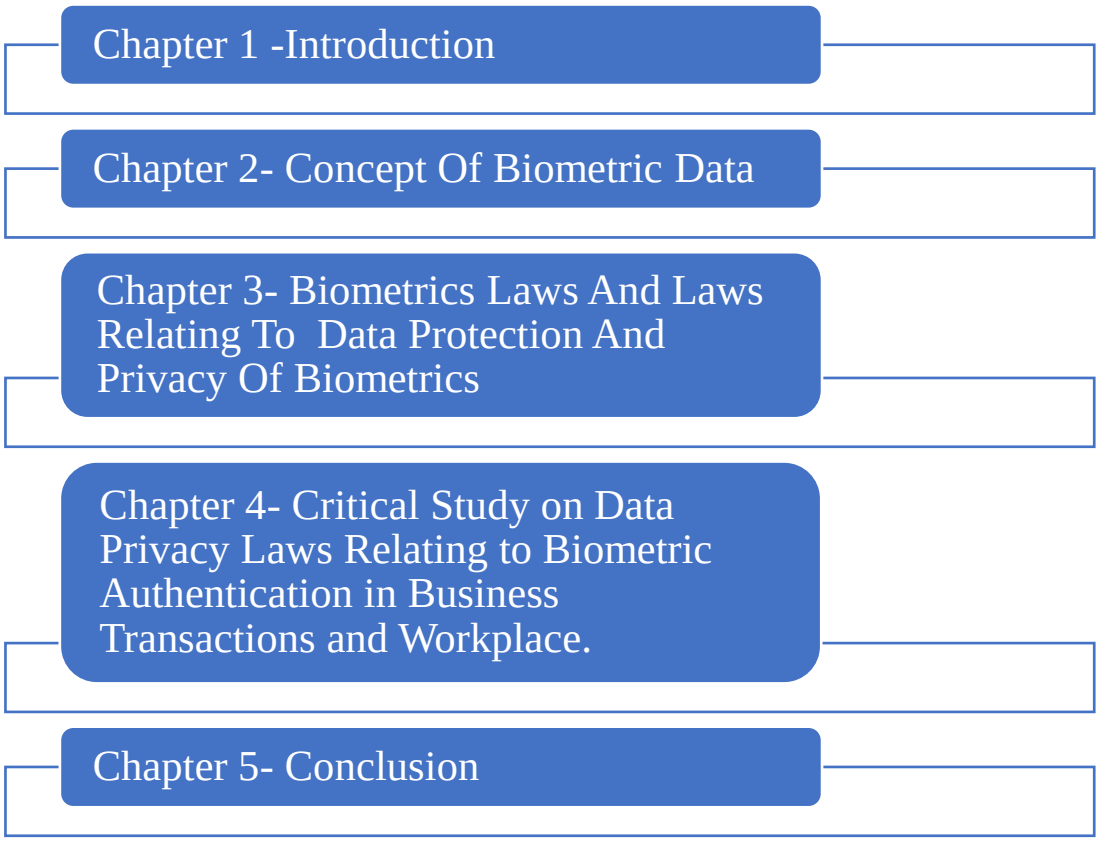
3 Whether the data privacy laws are comprehensive and sufficient enough for regulations of biometrics in business and workplaces in India?

4. Does the existing legislation of follow international standards in context of data privacy and biometric laws?

1.8 Research methodology

The researcher has used doctrinal research methodology to carry out the research of the current study. The methodology that has been adopted by the researcher mainly has been done through secondary sources. The proposed study will mainly use secondary sources such present legal statutes, books, journals, articles, online sources for research purposes and limit itself to materials available during the present situation. The proposed research follows an Analytical Methodology. The Researcher will refer to various statutory laws, notifications, compendiums and case laws relevant to the topic.

1.9 Research Design:



Chapter 1 : Introduction:

The chapter provides for an introduction to the dissertation and the purpose for which this research was undertaken. It provides for an appropriate background for the dissertation and contains the research methodology used for the research purposes of this dissertation.

Chapter 2 : Concept of Biometrics:

The chapter concept of biometrics provides for the meaning of biometrics and provides details on biometric data and biometric data systems and what are considered as biometric identifiers. The chapter also talks about the usage of biometric data in the present-day world in work places and business.

Chapter 3 : Biometrics Laws And Laws Relating To Data Protection And Privacy Of Biometrics

This chapter deals with the national and international laws and regulations that deal with biometric data. It also looks the laws on biometric data from the perspective of data privacy and protection. The chapter looks on the laws from the perspective of biometric data used generally in daily lives in workplace and business transactions and does not go into specific laws regarding biometric data use by the government, military, migration purposes and others

Chapter 4 : Critical Study on Data Privacy Laws Relating to Biometric Authentication in Business Transactions and Workplace

This chapter provides for the analysis and study of the data privacy laws of India in relation to biometric data in regard to their application in workplace and business transactions. This chapter analyses whether the present legislation marks up to the international standard set by other countries.

Chapter 5: Conclusion and Suggestions

This chapter concludes the dissertation and provides for certain suggestions and recommendations.

CHAPTER 2
CONCEPT OF BIOMETRICS

2. **Concept of Biometrics**

Technology has advanced rapidly over the years and use of biometrics in everyday life has become common place. Usage of Biometrics is not new and has been used in its crude form since ancient ages for contracts and business transactions by merchants and employers. They used to keep clay tablets with fingerprints or handprints and used them as authentication for contracts or worker identification. Biometric data relates to the biological data available from a person or an individual.

2.1 Meaning of Biometrics:

The etymology of the term Biometrics comes from the Greek Language. In Greek "bios" means life and "metric" means measurement. Biometrics in simple terms would then mean the measurement of life or measurements of the biological characteristics of a life person. "Biometric characteristics or identifiers are the physical, behavioural and physiological characteristics of a natural person. Biometrics is also considered as sensitive personal data by law in many countries, due to the data being extremely personal in nature .

Biometric characteristics are identifiers derived from a physical person that help to identify and verify the identity of a person. Biological characteristics such as eyes, fingerprints, voice, face, hand prints, palm prints, the gait of a person and others all are used in identifying an individual. Biometric data is the data collected from an individual of these physical and biological characteristics and stored and preserved in a data format. These data are used to then analyse and measure other biometric data of the same person at a later data in a biometric system where he will seek to authenticate or verify his identity. Biometrics of a person evolve over a time so they should be updated over time and corrected.

2.2 History of Biometrics:

The etymology of the term biometric arises from the combination of the Greek word 'Bios' meaning life and the word 'metrics' meaning to measure.[1] A simple system of using biometrics to identify human beings have been around for thousands of years.

i. Ancient Era:

"In many civilizations, fingerprints have been used as authentication to form contracts or were imprinted in clay tablets as a means of recognition. One of the oldest use of biometrics probably found are the cave paintings in France, believed to be at least 32,000 years old containing handprints of various people. Researches have felt that these handprints were probably used by the pre-historic men and women to identify themselves.[2]

The book called 'Jaamehol-Tawarikh' mentions using of fingerprints to identify people. It is a Persian treatise which was written by Khajeh Rashiduddin and Fazlollah Hamadani.

One of the oldest use of biometrics was done by the Babylonian King Hammurabi. Apparently, when King Hammurabi (1792-1750 BC) made his code of laws he used his right hand to authenticate the clay tablets on which the code of laws was written. Also, merchants used fingerprints to do business transactions and these were recorded on clay tablets. [3]

There has been documents and evidence that as far as 2000 years ago the Chinese used to use fingerprints and handprints for biometric authentication by pressing them in clay tablets and seals or papyrus. The Tang Dynasty period saw the use of handprints and fingerprints on contracts. At the end of written contract both the parties would

---

[1] Stephen Mayhew, History of Biometrics, BIOMETRIC UPTADE, (April 30, 2021, 8.29P.M) https://www.biometricupdate.com/201802/history-of-biometrics-2

[2] J. Clottes, Chavet Cave, (ca 30,000 BC), The Metropolitan Museum of art

[3] Els J. Kindt, Privacy and Data Protection Issues of Biometric Applications ,2013, A Comparative Legal Analysis, Law, Governance and Technology Series, (Volume 12, Springer, 2013) 1185

stamp their fingerprints on the contract. Even Chinese merchants as Joao De Barros mentions used fingerprints to settle contracts or agreements.[4]

ii. Scientific Era

"One of the important early works that discussed the use of fingerprints in differentiating human beings was that of Dr Nehemiah Grew. In his paper, "Philosophical Transactions of the Royal Society of London", published in 1634 he discussed extensively on using fingerprints to identify human beings. His work was carried forward later by numerous persons notably Govard Bidloo, Marcello Malpighi, Dr J.C.A. Mayer.[5]"

Purkinje was an anatomist who studied Dactyloscopy in the 1800's and he is the person due to whom in the 1880's the modern concept of using fingerprints to identify people geared notion.[6] He is known as the pioneer of the scientific system of biometric data that we use today. The Czech anatomist Johannes Evan-gelista Purkinje in 1832 designed a system of classification of fingerprints where he talked about nine fingerprint pattern types in his work and his research was done at the University of Breslau.[7]

"The system of using biometrics such as handprints was also used in India by the British officer Sir William Herschel to sign contracts with farmers.[8] Then in British India, seeing the work of Galton, Sir Edward Henry, the general inspector in Bengal collaborated with him to create the Henry Classification system, a method devised to easily

---

[4] Stephen Mayhew, History of Biometrics, BIOMETRIC UPTADE, (April 30, 2021, 8.29P.M) https://www.biometricupdate.com/201802/history-of-biometrics-2

[5] Stephen Mayhew, History of Biometrics, BIOMETRIC UPTADE, (April 30, 2021, 8.29P.M) https://www.biometricupdate.com/201802/history-of-biometrics-2

[6] A.K. JAIN, et al P. FLYNN & A.A. ROSS eds, HANDBOOK OF BIOMETRICS 1-22 (2nd ed Springer 2007)

[7] Rahul D Chaudhari, Ashok A Pawar &Rakesh S Deore, *The Historical Development Of Biometric Authentication Techniques: A Recent Overview*, Vol. 2 Issue 10, IJERT, 3921, 3922-3923 (2013)

[8] Rahul D Chaudhari, Ashok A Pawar &Rakesh S Deore, The Historical Development Of Biometric Authentication Techniques: A Recent Overview, Vol. 2 Issue 10, IJERT, 3921, 3922-3923 (2013)

store and classify fingerprints of people for their efficient and effective use.[9]"

"However, before the fingerprinting system became popular the concept or system of using biometrics to identify criminals was done by one Parisian police clerk and anthropologist named Alphonse Bertillon who in the year 1890 developed the system of Bertillonage, which used precise body measurements and classifications of a person along with marks such as scars, birthmarks and others to identify a person to use it in the criminal identifying system.[10] This system of criminal identification had many faults meaning that two persons may get different results while taking the measurements of two persons and there may be even false matching. This became absolutely apparent in the case of Will West who was convicted of a crime with the identity William West because the former was the twin of the actual offender.[11] Hence, attention was drawn into the fingerprint system."

" In the meantime, Francis Galton who had read on Dr Henry Faulds research on fingerprints took forward the idea of using of fingerprints to identify criminal in the 19th century, mainly because he researches yielded that fingerprint of each human being was completely unique, with no similarity between twins or triplets or others[12]. He is, in fact, the pioneer of the system of 10 fingers fingerprint classification system and he had found that only 1 out of around 64 billion may have similar fingerprints[13], making identification system of using fingerprints as identity attributes one of the most accurate systems."

---

[9] Rahul D Chaudhari, Ashok A Pawar &Rakesh S Deore, *The Historical Development Of Biometric Authentication Techniques: A Recent Overview*, Vol. 2 Issue 10, IJERT , 3921, 3922-3923 (2013)
[10] *Biometrics*, *History of biometrics*, HOMELAND SECURITY, (April 30, 2021, 8.00AM) https://www.globalsecurity.org/security/systems/biometrics-history.html
[11] *Biometrics*, *History of biometrics*, HOMELAND SECURITY, (April 30, 2021, 8.00AM) https://www.globalsecurity.org/security/systems/biometrics-history.html
[12] *Biometrics*, *History of biometrics*, HOMELAND SECURITY, (April 30, 2021, 8.00AM) https://www.globalsecurity.org/security/systems/biometrics-history.html
[13] Rahul D Chaudhari, Ashok A Pawar &Rakesh S Deore, *The Historical Development Of Biometric Authentication Techniques: A Recent Overview*, Vol. 2 Issue 10, IJERT , 3921, 3922-3923 (2013)

iii. The Present Era

"The 1900s ushered in a new era of revolution in the biometrics. This is the era that introduced facial recognition and iris pattern recognition.[14] "

"The concept of iris pattern recognition was put forward by Frank Burch, an American ophthalmologist and later in 1960, a company in Palo Alto, California used machine for facial recognition for the first time. This was a pioneering movement for automated biometrics."

" The year of 1965 saw the development of the first system to recognise signatures by the North American Aviation and again in the year 1974, the University of Georgia made a major breakthrough by using a system able to recognise hand geometry."[15]

"In the meanwhile, FBI had begun using fingerprint identification system and moreover work progressed on automated facial recognition, an exceptional contribution was made by researchers L.D. Harmon, A.J. Goldstein and Lesk who analysed around 21 special facial markers for the task."[16]

"Also, the very basic model of speech recognition system was being made by Dr Joseph Perkell and later in 1976, Texas Instruments was credited with making the first prototype of a speech recognition system, which was again later studied upon by NIST Speech Group.[17]

At this stage, we see that most concepts of biometrics that we use in the modern-day such as fingerprint recognition, speech recognition, facial recognition and others have started to come together. Law enforcement and government agencies have also started using

[14] *History of Biometrics*, REFACES.COM, https://recfaces.com/articles/history-of-biometrics (May 1 2021, 8.00AM)

[15] Rahul D Chaudhari, Ashok A Pawar &Rakesh S Deore, *The Historical Development Of Biometric Authentication Techniques: A Recent Overview*, Vol. 2 Issue 10, IJERT , 3921, 3922-3923 (2013)

[16] Rahul D Chaudhari, Ashok A Pawar &Rakesh S Deore, *The Historical Development Of Biometric Authentication Techniques: A Recent Overview*, Vol. 2 Issue 10, IJERT , 3921, 3922-3923 (2013)

[17] *History of Biometrics*, REFACES.COM , https://recfaces.com/articles/history-of-biometrics (May 2, 2021, 8.00AM)

biometrics and in the year of 1992, the NSA formed a consortium consisting of academicians, government agencies, private members from commercial and other industries to form the Biometric Consortium.[18] This led to a new digital and automated biometric system and standards that we see now. FERET (Face Recognition Technology Evaluation) 1993- 97, then IAFIS (Integrated Automated Fingerprint Identification System), Human Authentication API- an SOP one of the very firsts of protocols of biometric standards, that set the standard for commercial and generic biometric to be used in the market and the study by International Civil Aviation Organization on the compatibility of biometrics with MRTD process to use biometrics as an identification method for international standard opened the doors for biometrics system and biometric authentication and identification that we have at the present.[19] "

2.3 Present concept of Biometric Data System

2.3.1. "Biometric Data"

"Biometrics are the biological characteristics of a natural person. However, for authentication, verification or identification purpose such biometrics must be rendered in a form that is accessible or provides the ability to provide the above functions. The data of biometrics so being collected is called "Biometric Data" and they refer to physical or physiological or behavioural unique identity attributes of a human being collected as data through a biometric system.[20] While in olden days the collection of biometric data and verification was manual and tiring, nowadays collection, retention, storing and handling of biometric data is done by machines. The system is automated and the Biometric data are

[18] *History of Biometrics*, REFACES.COM, https://recfaces.com/articles/history-of-biometrics (May 2, 2021, 8.00AM)

[19] *History of Biometrics*, REFACES.COM, https://recfaces.com/articles/history-of-biometrics (May 2, 2021,8.00AM)

[20] Rahul D Chaudhari, Ashok A Pawar &Rakesh S Deore, The Historical Development Of Biometric Authentication Techniques: A Recent Overview, Vol. 2 Issue 10, IJERT , 3921, 3922-3923 (2013)

stored in digital form. [21] Biometric identifiers are fingerprints, iris, DNA, hand vein patterns and others. [22] These biometric identifiers are first scanned and fed into a biometric system which stores it in form of digital data. These data are called biometric data of a person and is created by making profile from the samples of biometric data received from a natural person. The automated system can easily sore data, preserve it and disseminated it across various channels. Biometric data is mainly favoured because of its uniqueness, as no other individual will be able to access or duplicate a biometric data."

2.3.2. What is biometric system?

"Biometric systems are nowadays basically automated systems that are able to authenticate and identify a person using biometric data such as fingerprint, iris recognition , DNA and many others. The systems recognise or authenticate data my matching the current data with the previous information put in the database. The systems can be varied; they can be a simple system capable of recognising one biometric characteristic to complex systems that is able of recognising multitude of characteristics or biometric data.[23] The systems use mathematical, technological and statistical applications and programmes to perform their functions and verify or authenticate the data. These data are generally called a biometric modality, that is chosen as one modality but generally a combination of modalities to represent the profile of a person depending on the purpose such data is collected. There is a need to understand which characteristics or modalities are fit to be used in automated biometric systems as nowadays everywhere these automated systems are used to verify and authenticate data. Biometric modalities that are fit to be used in systems must contain some special characteristics. The modalities or biometric characteristics that will be used as people characteristic must contain certain features. They are :

[21] Rahul D Chaudhari, Ashok A Pawar &Rakesh S Deore, The Historical Development Of Biometric Authentication Techniques: A Recent Overview, Vol. 2 Issue 10, IJERT , 3921, 3922-3923 (2013)
[22] Rahul D Chaudhari, Ashok A Pawar &Rakesh S Deore, The Historical Development Of Biometric Authentication Techniques: A Recent Overview, Vol. 2 Issue 10, IJERT , 3921, 3922-3923 (2013)
[23] United Nations Compendium of recommended practices for the responsible use and sharing of biometrics in counter-terrorism, 2018, United Nations Office of Counter -Terrorism (UNOCT), Counter-Terrorism Committee Executive Directorate (CTED), Biometrics Institute.

i. “Universality-

The biometric characteristics must be universal in nature meaning that the characteristics from which data is to be taken must be able to be found in all human beings in the world. The requirement on universality of data excludes any specific traits a human being may have such as beauty spots, or scars or stains, or any bodily mark that works as an identifier because not all human beings may have them. For example, people of certain ethnicity or place may have a specific trait that other people don’t have like freckles. Even, then many people may due to sickness or accident or disfigurement or disability lose one or two biometric characteristics. Like a person may lose his hand or leg and the most common biometric identifier the face may be scarred. Biometric systems being automated systems when they will match a scarred face of a person with an unscarred face of the same person may give negative match. In case of lost hand or foot a person may not be able to use biometric system. As, it is a biometric system may not be accessible for all persons and when making biometric regulations these points should be taken into account.

ii. Unique-

One of the most important features that a biometric characteristic should have that they should be unique to every person and they must not be generally the same. This principle excludes into facial image consideration identical twins and identical siblings. However, even then the fingerprints of identical twins are usually different from each other. Only Biological characteristics that have the most negligible chances of two persons possessing same features and only they can be used in biometric applications or systems. In case of identical twins, although they may share same face or DNA, they will have different fingerprints or even signatures. This characteristic of uniqueness is very important and necessary as biometric data are used to verify and authenticate the identity of the people.

iii. Permanent and persistent:

Biometric characteristics that are chosen to be collected to fit into applications to verify or authenticate must have the feature of permanency and persistence in nature; meaning that the data that would be collected should remain unchanged over a period of time. It cannot be fast changing or completely changing biological data. It must be something of a permanent nature that remains relatively unchanged throughout a person's lifetime. The height of a person cannot be biometric data because it may change within a few years. If any characteristic that is constantly used than it would create a lot of hassle.

Fingerprints and iris recognition along with DNA are the biometrics that are said to remain almost completely constant during a person's lifetime, except for a few major changes. Facial recognition although a viable and easy to collect biometric characteristic is only semi-permanent. Facial image as biometric data would need constant maintenance as humans age. When a person is a child his facial features are different and quickly keep on changing within months or one to two years; while in adulthood the facial image gains stability over a period during youth because although the face is changing, the structure is set and remains the same. Again, in old age wrinkles set in face and it sags and then the face changes. Also, if a person wears make up or grows beard or wears glasses the system may not recognise them.

Hence, it is important to have stable biometric identifiers form biological characteristics. It is necessary because the selection will also affect the security of the data. If the data is unreliable there may be data breach and if a person has been rejected because the biometric system sent out a negative report on verification of identity because of the use of false and unstable identifiers then additional checks have to be made which will then waste a lot of resources as well as waste a lot of time.

iv. Collectible and accessible:

Biometric data must be such which is easily collectible and usable. It means that the biometric data so collected can be easily obtained without much fuss and can be converted into digital form of data capable of verifying the identity of an individual. The data should also be able to be easily retrieved when needed and be usable. Fingerprints or facial image or iris scan are easily collectible and they can be formed into data easily and used. All in all, the it should be user friendly. Accessible means that the information so collected must be able to be accessed form a particular database without interferences.

v. Acceptable:

"One of the most important features of biometric modality is that they must be such that the society does not find it objectionable in giving such data to the government or put it in public and they must be capable of such that they can be used by a majority of the population."[24]

vi. Performance:

Identification and verification of persons in today's world needs to be fast and effective. So, the biological characteristics collected or chosen as fit for application for verifying or authenticating identity must be such data when inputted into a biometric system is be able to perform fast and effectively. For illustration, fingerprints or facial image depending on the speed of the system can perform effectively and when such data can quickly be processed.

vii. Reliability:

The most important characteristic that a biometric identifier should have is that it should be reliable, meaning it should not be able to be forged.

The characteristics should be such that they are not capable of defrauding the system or circumvent it.

[24] United Nations Compendium of recommended practices for the responsible use and sharing of biometrics in counter-terrorism, 2018, United Nations Office of Counter -Terrorism (UNOCT), Counter-Terrorism Committee Executive Directorate (CTED), Biometrics Institute.

2.3.3.Types of Biometric Data:

The Biometric Institute provides certain biometric data types that are common in todays' world and is useable as biometric data. They are DNA Matching- a sample of DNA is collected from the person and that sample's analysis is stored in digital for further match in the future, retina and iris recognition of the eyes , face recognition, fingerprint recognition, finger geometry recognition, ear recognition, vein recognition, behavioural aspects like gait recognition and keystroke recognition, others such as voice recognition and speaker identification and authentication, hand-geometry recognition, the very commonly used signature recognition. [25]

2.3.4 Biometric authentication and identification :

Biometric authentication and identification are basically the process of authenticating biometric details of a person to match his identity to the profile already in a system to allow him access to any document or area or use for any other purposes like government id card, etc. Generally, the system works in two ways, one is physical authentication and one is distance authentication. Physical authentication and identification are done through present biometric devices such as fingerprint scanner, facial recognition machine, iris scanner and others wherein the person himself is physical present and scans his biometrics at that point of time. This maybe done so to let him access something at the present time . An example is using fingerprint scanner to unlock a laptop. Distance authentication is generally done to identify the profile and collect and match data, example a bank may ask for biometric authentication card or number to verify whether you are the actual holder of your personal details and verify the identity of the person. Biometric data and authentication are being used largely in the present world.

[25] *Types of biometrics*, BIOMETRICS INSTITUTE, https://www.biometricsinstitute.org/what-is-biometrics/types-of-biometrics/ , (July 31, 2021 8.29 PM)

2.3.5 : Usage in Workplaces and Business Transactions:

I. General usage

"At present, there is a universal use of Facial, image fingerprints, voice recognition, speech recognition and signature recognition in normal life of almost all individuals on the planet. Google, which is one of the prime technology platforms practices user voice recognition as one of the approaches to permit people to search data, give instructions and perform other functions. Countless other technology platforms and sectors have been seen incorporating biometric authentication in the 21st century. The first to use biometric data system was government agencies mainly the law enforcement sectors in prison systems, military access controls, criminal identification along with civilian identification especially in the United States of America.[26]

"The present century has seen overwhelming growth and spread of usage of biometrics. Many sectors have started using them especially the government agencies, law enforcement agencies, intelligence bureaus, health care sectors for civilian identification, criminal identification, military for identification the armed forces and access control, banking sectors for customer and business identification, commercial industries, healthcare sectors, mobile and laptops and many others."

i. Use by the Government , military or other law enforcement agencies:

In USA, use of biometrics has become the norm for everyone. The social security card that is f Let's consider the case of USA for instance, the FBI and other agencies have been using various types of biometric data sample of biometric profile for identifying and tracking criminals, especially the building of an IAFIS by Lockheed Martin for the FBI in the year 1994.[27] After the incident September 11 in 2001, security in the States further increased with the founding of NBSP or National Biometric

[26] Rahul D Chaudhari, Ashok A Pawar &Rakesh S Deore, The Historical Development Of Biometric Authentication Techniques: A Recent Overview, Vol. 2 Issue 10, IJERT , 3921, 3922-3923 (2013)
[27] Rahul D Chaudhari, Ashok A Pawar &Rakesh S Deore, The Historical Development Of Biometric Authentication Techniques: A Recent Overview, Vol. 2 Issue 10, IJERT , 3921, 3922-3923 (2013)

Security Project to develop modern biometric techniques.[28] They even managed to locate one terrorist from the incident using biometric who was a part of planning the 9/11 incident. The EU also requires biometric authentication and registration of civilians for availing government facilities. Biometric registration is completely present in countries like USA, China, Japan, Russia and many other countries.[29] Biometric authentication and identification is also associated with Government IDs and social security system and European countries, along with countries like USA, China, and many other countries use biometric data such as fingerprints, facial recognition, palm print, signature recognition for issuing IDs such as Driver's License, social security card, Bus Card, and others. EU is known for 'ePass' to its citizens under the rules of EU Council Regulation and biometrics play an important role in such ePass. Biometrics is used in border and migration as well as visa and passport. Generally, people used facial recognition and fingerprint recognition in passports. Meanwhile in borders generally facial recognition and digital photo is done along with finger prints especially in USA borders, with the intent to track criminals, counter terrorism and to avail the people security features.[30] Even the UN in the prepared CTED document 'Compendium of Recommended Practices for the Responsible Use and Sharing of Biometrics in Counter-Terrorism' emphasizes the use of biometric authentication and identification in a safe manner to track terrorists and counter terrorism. For example, International Terrorist Osama bin Liden's bodily remains was identified and authenticated by CIA in 2011 using biometric data i.e., through his previously recorded

[28] Rahul D Chaudhari, Ashok A Pawar &Rakesh S Deore, The Historical Development Of Biometric Authentication Techniques: A Recent Overview, Vol. 2 Issue 10, IJERT , 3921, 3922-3923 (2013)
[29] Mehedi, *25 Uses of Biometric in Today's Society*, BIOMETRICTODAY, (April 30, 2021, 8.00AM) https://biometrictoday.com/uses-of-biometric-technology-today-society/
[30] Busch, Christoph. *"Facing the future of biometrics. Demand for safety and security in the public and private sectors is driving research in this rapidly growing field."* Vol 7 Spec No EMBO reports, S 23-5. (2006) doi:10.1038/sj.embor.7400723

DNA sample and facial recognition.[31] It is not only the Government, military or law enforcement that uses biometrics for security, welfare schemes or tracking of criminals.

ii. Usage in businesses, commercial sectors and workplaces

Biometric authentication and identification system is used largely in banking sectors and in commercial transactions. Banks collect our photo, digital and otherwise, signature and thumbprints for general transactions and such data are recorded in the system of banks. Nowadays banks have facilitated mobile or e-banking apps and encouraged its use by customers. Such apps are generally found to record our biometric data. Also, payment apps or platforms that use payment gateways have been found many a times to use and encourage biometric authentication and identification for allowing access to such platforms and then allow users to confirm transactions. We can take the example of GPay, PayPal, Paytm, BHIM Upi or others where we can scan our fingerprints in the app, they will record the data and then allow future transactions and access to any of our data in the app after verifying our fingerprints and authenticating them. This is so also for many apps that allow commercial transactions such as Amazon, and other apps. Banks also use biometric authentication for secure vaults and lockers for customers. And even banking personnel has to use biometric banking for secure access in certain cases. In many countries bank accounts are linked to government ids that use biometric system, such as the United Kingdom and countries in EU. EU also requires incoming students from other countries to update their biometrics with respective townhalls of their residing town or the town of their colleges.[32] We often see work places and offices using biometric system such as punch machines that use fingerprints to record attendance. It has been the practice

[31] *History of Biometrics*, REFACES.COM, https://recfaces.com/articles/history-of-biometrics (May 2, 2021, 8.00AM)

[32] EMN SYNTHESIS REPORT – IMMIGRATION OF INTERNATIONAL STUDENTS TO THE EU, European Migration Network Study 2012

of many industries and companies to secure their workspaces, factories, documents and other high-security areas and things by using biometric authentication of iris recognition, facial recognition and thumb print registration to allow access only to authorized personnel and prevent such data from theft and misuse. Nowadays it is common for government offices, schools, colleges, workplaces, factories and others to use punch machines and other biometric system to allow access to facilities and to register attendance. Also, nowadays most hospitals and healthcare facilities link their patients' files with their government ids that use biometric authentication. At this juncture we can't forget to talk about researches, scientific and technological developments, research laboratories and high-security documents and documents of national security which are protected by using biometric systems and authentication to allow only registered and authorized personnel to access the data and the information.

While we talk about biometric authentication and identification, we must talk about the present generation of smartphones, laptops, computers, AI operated systems and others. The smartphones now are biometric enabled which uses facial recognition and fingerprint recognition to allow users access to the phone, enhancing security since no one else than the user can unlock the phone and access its contents. Technology companies are also rapidly producing laptops and PCs that use facial recognition and fingerprints for biometric authentication and recognition. We have Apple's MacBook Pro using fingerprint recognition system to unlock the MacBook by using Apple ID and Apple Pay; same ways we have other laptop companies such as Lenovo which use FIDO (Fast Identity Online), HP, Samsung and DELL which use fingerprint authentication and facial recognition. We are also increasingly using home security features such as doors and locks that use either fingerprint sensors, facial recognition or

voice recognition to allow entry or unlock the doors. [33] With the launch of technologies such as SIRI, Google voice and speech recognition technologies, ALEXA have used these technologies that store our private data along with our biometric data to operate a lot of our home and offices appliances, our documents, our accounts, to do shopping, operate cars, machines and many others. We can ask Alexa to buy a product from amazon with just one voice command or ask Siri to send an email. Also, nowadays entrance examinations also use biometric data to ensure that the candidates appearing in the exam are the legitimate candidate themselves. As we can see that biometric system has completely percolated into our daily lives everywhere from banks to schools, to academics to workplaces to government and everywhere. Such percolation in our daily lives require certain measures and regulations so that such data are not misused.

[33] Mehedi, *25 Uses of Biometric in Today's Society*, BIOMETRICTODAY, (April 30, 2021, 8.00AM) https://biometrictoday.com/uses-of-biometric-technology-today-society/

CHAPTER 3

BIOMETRICS LAWS AND LAWS RELATING TO DATA PROTECTION AND PRIVACY OF BIOMETRICS

Nowadays, usage of biometrics of a person is extremely common and widespread for different purposes all over the world be it for government use, military use, business use or use of "Biometric Data" of person in workplace. The automated "Biometric Data" system is the prevalent system is nowadays world and the data generated is stored digitally as "Biometric Profiles" or logs in cloud or data centre. Considering, that "Biometric Data" are extremely personal and sensitive in nature being completely unique to one person, it is very necessary that such "Biometric Data" is handled properly and not misused. Also, there needs to be a set standard of what type and which kind of "Biometric Data" will be accepted as legal biometrics of a person. For illustration, if the iris scan of A does not produce a clear iris pattern that is distinguishable and is a bit unclear, such iris scan of person A should not be acceptable as it will not yield a correct data for future uses. Hence, it is necessary to set standards for acceptable "Biometric Data". Also, there are various machines or systems which collect "Biometric Data" throughout the world and it is necessary that there is uniformity in the standards of each system. Hence, considering all factors most countries have made regulations regarding biometrics. There are even some international and national bodies and institutions regulating "Biometric Data", their usage, protection of such "Biometric Data" and others.

3.1. Regulatory Institutions:

There are many bodies in the world that regulate biometrics. A few of them has been provide below to understand the aspects regarding "Biometric Data" that needs regulations.

i. Biometric Consortium by NSA

It is one of the oldest bodies regulating the use of "Biometric Data" and it was formed by the National Security Agency or NSA on the direction of the Government of USA along with the National Institute

of Standards and Technology or NIST. The main focus of the Consortium for the Government of USA was to serve as research centre on the development, evaluation, test and application of biometric authentication technology.

The first meeting of the Biometric Consortium was on October 1992 and Dr, Benincasa was the chairman. The main objective of the meeting was to become a space for sharing and exchanging information on biometrics among the government, academia and industry. In 1994, the chairmanship of Biometric Consortium was given to Dr Campbell and in December 7, 1995 the charter of the Biometric Consortium was formally approved. The charter laid down the mission of Biometric Consortium.

The mission of Biometric Consortium was laid down in a few points by the charter[34]. A few of them have been given below.

- It serves as a research centre for the Government for biometric authentication technology and their development and application
- One of its main mission was to encourage usage and acceptance of biometric technology and to make usage of biometric technology efficient and cost effective and unique.
- To be a place of sharing and exchanging information on biometric technology between industry, government and academia.
- To promote biometric technology and create standards on testing databases, procedures and protocols regarding “Biometric Data” for the community
- To also address the legal , safety, performance and ethical issues surrounding biometric technology.
- To establish required and needed ad hoc bodies to address the need of any arising issues within the Government biometric community

[34] Biometric Consortium, http://www.biometrics.org/, https://web.archive.org/web/20060401033426/http://www.biometrics.org/links.html (July 10, 2021)

These were the few points of the mission of Biometric Consortium. The Biometric Consortium mainly works within the USA and every year they hold a conference cum expo to talk on the new developments on biometric technology and law.

ii. European Association for Biometrics or EAB:

It is based in Europe and is a non-profit and nonpartisan association which works biometrics and on digital identity.[35] The main mission is geared towards serving the citizens of Europe by handling the complex issues regarding digital identity in Europe whether the issues be in context of privacy, migration, welfare scheme and others. They are responsible for promotion of accountable use of digital identity system and adoption of such modern digital identity systems. The association interacts with and supports governments, associations, NGO's, businesses, industries, and academia on matters regarding biometrics. It strives for ensuring that biometric identity systems are private, secure, safe, fair and accessible in Europe.

iii. Biometric Institute:

Biometric Institute is one of the most popular institute regarding biometrics and it is an international organisation and forum for users of "Biometric Data" and other parties. The institute was founded on 11th October in Australia in collaboration with the Australian Taxation Office, Federal Police and others.[36] The Biometric Institute is in fact one of the leading international organisations in the world which lays major emphasis the proper use of biometrics by laying down of standards, proper procedures, rules and regulations and by doing their utmost best that use of "Biometric Data" is done in a way that does not adversely affect the human rights of individuals or others. The Institute is also the authority on what kind or type of data

[35] European Association For Biometrics, About, https://eab.org/ (July 15,2021)
[36] Our History, Biometrics Institute, https://www.biometricsinstitute.org/about/our-history/ (July 15, 2021)

is considered as "Biometric Data" and what are the standards regarding such "Biometric Data". They are also responsible for sharing knowledge to many nations building a huge network with a representative of more than 800 individuals, 204 organisations, and 24 countries. The Biometric Institute follows four main values firstly being trustable meaning being committed to transparency, fairness, integrity and honesty; secondly being impactful by leading pioneering change and innovation; thirdly being collaborative with different stakeholders and fourthly and most importantly accountability.[37] The main mission of the institute is to promote the ethical, fair, transparent and responsible use of "Biometric Data" and biometric technologies among others and to act as a connector to all stakeholders that use "Biometric Data". The Institute even lays down privacy guidelines that data controllers who handle "Biometric Data" should follow and include in their privacy policies.[38]

iv. International Biometric Industry Association or IBIA

This association is concerned with the ethical and appropriate use of biometric technology in identity management regarding industries and businesses. Founded in September 1998 by the people in Washington D.C. the main goal of the association is to ensure like all other organisations the safety, security, efficiency, privacy and suitability of use of "Biometric Data" for authentication purposes in regards to governments, individuals and businesses.[39] The way they maintain their mission is by focusing on the focal points of education, advocacy and connections. The association works mainly on projects regarding privacy, cybersecurity, border issues, migration and others

[37] Our Values, Biometric Institute, https://www.biometricsinstitute.org/about/our-values/ (July 17,2021)
[38] Privacy and Biometrics, Biometric Institute, https://www.biometricsinstitute.org/what-is-biometrics/privacy-and-biometrics/ (July 17,2021)
[39] John Trader, June 17, 2016, The Top 5 Biometric Associations and Regulatory Bodies Around the World, M2SYS BLOG , https://www.m2sys.com/blog/biometric-hardware/top-5-biometric-regulatory-bodies/ (July 17,2021)

Another regulatory body that attempted standardisation of “Biometric Data” and system was by the ISO when it established the committee ISO/IEC JTC1 Subcommittee 37 (JTC1 /SC37)’ whose purpose was to standardise the technologies used in biometric system and “Biometric Data”. As such there are many regulatory bodies that has tried to promote accountability and fair use of “Biometric Data”. The main aim of all the institutions and regulations has been to form a space that can oversee the advent and development of biometric technology and the influence of it on daily lives and to find solutions and guidelines to the issues surrounding “Biometric Data”. The institutions are also concerned with human rights and safety, security and privacy of “Biometric Data”. In concern with the above various countries have also made laws on the “Biometric Data”.

3.2. Laws on Biometrics and Data Privacy around the World:

Nowadays, most developed and developing countries use biometric authentication as means of identifying individuals. “Biometric Data” is used to create a profile of a person which then serves as sort of digital and biometric identity for the person. In many countries the identity card of a person holds the chip that also contains a “Biometric Profiles” of the person. To access any services whether from the government or certain welfare schemes the person has to authenticate their biometrics at the authentication point and only when the profiles are a match then the person will be able to access services. In workplaces, institutions and even in business transactions use of “Biometric Data” to authenticate identity has become largely commonplace. Hence to ensure that “Biometric Data” is used in an ethical manner and not misused there is need for legislation. Since, “Biometric Data” is considered to be extremely personal data or sensitive data it is necessary to ensure the protection and privacy of such data. Here, we will simply deal with regulations around the world that provides for data privacy and laws regarding “Biometric Data” in a general manner. We won’t deal with laws regarding biometrics and its uses in immigration laws, passport laws, military laws or laws related to the security of

a country except for United Nations compendium on use of biometrics for the purpose of counter-terrorism for the reason that it provides an insight on biometrics and data privacy.

A. USA:

The United States of America unlike other countries does not have one comprehensive biometric law relating to data protection or privacy that applies to the whole of the nation. However, many states of USA have adopted and passed different laws regarding biometrics and data privacy mainly concerned with biometrics. Although US other states have comprehensive data privacy laws , we won't be dealing with them as they deal with all data in general and not "Biometric Data" in specific. The US states that currently have Biometric Privacy Laws are Illinois, Texas, Washington, California, Arkansas, and New York.

i. Illinois Biometric Privacy Information Act or BIPA:

The BIPA is one of the oldest legislations regarding biometrics in the USA and it was enacted in the year of 2008 mainly to promote the ethical and responsible use of biometrics by regulating the collection of "Biometric Data", by regulating the procedures related to the disclosure of such collected "Biometric Data" and by providing for the destruction of such collected "Biometric Data".[40]

The main point of the Act is that it prescribes for procedures and rules on how "Biometric Data" is collected and handled by private entities who collect and store such data from individuals.

The BIPA Act provides in Section 15 about the retention, collection, disclosure and destruction of "Biometric Data". It provides that any private entity that wants to collect biometric information must develop a written privacy policy where they will specify the retention schedule of the "Biometric Data" and also provide for the guidelines for permanently destroying the "Biometric Identifiers" of an

[40] AMBA KAK, ed., REGULATING BIOMETRICS: GLOBAL APPROACHES AND URGENT QUESTIONS,52-62 (Al Now Institute, 2020), https://ainowinstitute.org/regulatingbiometrics.html.

individual after the purpose for which it has been collected is satisfied or within a period of 3 years after an individual has interacted with entity.[41] This sub-section deals with the principle of "Right to be Forgotten" of "Biometric Data" where a person has the right to have his "Biometric Identifiers" or profile completely and permanently erased from the database of a private entity. The Act also provides any private entity before collecting, purchasing or capturing any "Biometric Data" of any individual must inform the concerned individual or his representative and get his informed and free consent, inform the individual or his representative on why and for how long such "Biometric Data" is needed and only when the private entity receives a written consent or release he can collect the "Biometric Identifiers" or data of the individual.[42]

Here, the Act is concerned with the privacy rights of the individual and the private entities must get informed consent by the individual before collecting and circulating the "Biometric Data" of such individual. One of the main features of this Act is that it stops the private entities from profit mongering by stopping them from selling "Biometric Data" for profit and hence taking a step towards maintain the privacy of the "Biometric Data" collected from individuals. A private entity is banned from selling, trading, leasing or by any means

[41] Note- Biometric Information Privacy Act., 740 Ill. ICLS. 14/15 ("§15 (a) A private entity in possession of "Biometric Identifiers" or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying "Biometric Identifiers" and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first. Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a private entity in possession of "Biometric Identifiers" or biometric information must comply with its established retention schedule and destruction guidelines.)

[42] Note- Biometric Information Privacy Act., 740 Ill. ICLS. 14/15 ("§15 (b) No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's "Biometric Identifiers" or biometric information, unless it first:

(1) informs the subject or the subject's legally authorized representative in writing that a "Biometric Identifiers" or biometric information is being collected or stored;

(2) informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a "Biometric Identifiers" or biometric information is being collected, stored, and used; and

(3) receives a written release executed by the subject of the "Biometric Identifiers" or biometric information or the subject's legally authorized representative

profiting from a client's "Biometric Data" that they are in possession of, meaning any organisation or business cannot sell or trade or lease the "Biometric Identifiers" of their clients or customers to make profit.[43] Even if a private entity were to disclose any "Biometric Data" to any other entity the individual whose "Biometric Identifiers" will be disclosed must be informed for what purpose and how long his "Biometric Data" will be shared and he or his legal representative must give informed consent for such disclosure, the exception is for any disclosure related to any financial transactions for which consent was obtained before, disclosure is required by law or the court.[44] The BIPA holds a standard for data privacy and protection procedures to be maintained by the private entities when dealing with "Biometric Data". It put emphasis on that a private entity must store, collect, transmit and protect "Biometric Data" from all disclosure and treat it as confidential and sensitive information. In Illinois many cases have been brought under the BIPA alleging privacy harms such as breaches of data, unconsented surveillance, or disclosure of sensitive information. One of the key features of BIPA is that it does not follow the line of thought that malicious harm must occur for there to be an infringement of rights, it follows the principle that whether any malicious harm was done or not with the "Biometric Data" collected; however, if such data was collected or processed without explicit consent of the person and any prior notice given, then such action was

[43] Note- Biometric Information Privacy Act., 740 Ill. ICLS. 14/15 ("§15 (c) No private entity in possession of a "Biometric Identifiers" or biometric information may sell, lease, trade, or otherwise profit from a person's or a customer's "Biometric Identifiers" or biometric information.)

[44] Note- Biometric Information Privacy Act., 740 Ill. ICLS. 14/15 ("§15 (d) No private entity in possession of a "Biometric Identifiers" or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's "Biometric Identifiers" or biometric information unless:

(1) the subject of the "Biometric Identifiers" or biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure;

(2) the disclosure or redisclosure completes a financial transaction requested or authorized by the subject of the "Biometric Identifiers" or the biometric information or the subject's legally authorized representative;

(3) the disclosure or redisclosure is required by State or federal law or municipal ordinance; or

(4) the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

enough to cause breach of the law and affront to the autonomy of the victim.

Such was in the case of Rosenbach v. Six Flags Entm't Corp[45]. , where a claim was brought into the court by the mother that the amusement park collected her minor child's fingerprints for their system without her consent. Here the Supreme Court of Illinois held under BIPA the above company violated the person's right to privacy to control who had access to their biometric identification and who are the "Biometric Identifiers" that they will share their own biometric identification. We can also see the recent case of Clearwater AL which accessed more than three billion images of people without their express permission and found themselves in huge trouble and in 2020 had to end all its contracts with all agencies that were not involved in law enforcement in Illinois.[46] As such we can see that BIPA has a strong standard protection of privacy and protection of data regarding biometrics.

ii. Texas Capture or Use of "Biometric Identifiers" Act (CUBI) :

The Texas CUBI is a very important Act of Biometrics because it mainly deals with businesses and organisations in Texas that collect or use "Biometric Identifiers" or data. CUBI was enacted in 2017 and mainly applies to collection of "Biometric Data" by entities for commercial purposes.[47] Similar to BIPA, CUBI requires a company to provide a notice and then obtain the individual's consent to capture "Biometric Identifiers" of that person. Also, the companies must permanently destroy the "Biometric Identifiers" within one year of finishing or completing the initial purpose for which the data was

[45] Rosenbach v. Six Flags Entm't Corp., 2019 IL 123186, ¶ 8, 129 N.E.3d 1197, 1200–01

[46] Ryan Mac, Caroline Haskins, and Logan McDonald, "Clearview AI Has Promised to Cancel All Relationships with Private Companies," BUZZFEED,), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-no-facial-recognition-private-companies, (July 20, 2021)

[47] Texas Lawyer, October 5 2020, Meet CUBI—What Companies Need to Know About Texas' Biometric Privacy Law, BLANKROME, https://www.blankrome.com/publications/meet-cubi-what-companies-need-know-about-texas-biometric-privacy-law (July 23,2021)

collected. Such as in business workplaces, after an employee quits or leaves the organisation his ""Biometric Profiles" must be deleted. Businesses and companies are prohibited from selling, trading, leasing or disclosing the "Biometric Data" of a person to third party unless express consent is given or it is required in due course of financial transaction or disclosure of such "Biometric Data" is required or permitted by the law or the court. Also, the "Biometric Data" must be handled in a reasonable manner as one would protect "sensitive personal data". The power to enforce the Act lies upon with Texas Attorney General. In late 2020 the Office of the Texas Attorney General was investigating Facebook as it was alleged for unethical and improper biometric practices.[48]

iii. Washington House Bill 1493 (2017):

The above legislation also known as "Wash .Rev. Code Ann §19.375.020" is a rule which prohibits any business or company or any legal entity from inputting or entering ""Biometric Profiles" or data of any person "in a database for a commercial purpose, without first providing notice, obtaining consent, or providing a mechanism to prevent the subsequent use of a "Biometric Identifiers" for a commercial purpose."

The other Biometric Laws of California, New York and Arkansas also like the above three laws deal with the retention, collection , storage , transmit, protection and disclosure of "Biometric Data". The California Consumer Privacy Act 2020 expanded the definition of "Biometric Data" to include physiological, behavioural, biological characteristics that can be used to establish the identity of a person. Slowly, but surely other states of the USA are also implementing separate laws on "Biometric Data".

[48] Texas Lawyer, October 5 2020, Meet CUBI—What Companies Need to Know About Texas' Biometric Privacy Law, BLANKROME, https://www.blankrome.com/publications/meet-cubi-what-companies-need-know-about-texas-biometric-privacy-law

B. Europe:

One of the most stringent and developed laws regarding data protection and biometric laws in the world is the "GRPR" or General Data Protection Regulation of the European Union. However, before "GRPR" was enacted in May 25,2017, the important regulations regarding biometrics were given by 'Data Protection Working Party'. We will not deal biometric laws nation by nation but as whole of European Union. The 'Data Protection Working Party' set forward important guidelines on August of 2003. " In its opinion WP 80 focused mainly on the verification process of "Biometric Data" rather than on the aspect to gain control or access through "Biometric Data" implicitly pointing out that biometric system should mainly be used for verification purposes. The Directive 95/46/EC also sets forth principles regarding data quality which states that personal data must be kept modernised when essential and must be true.[49] Two of the most important principles regarding "Biometric Data" was given by Article 29 of the Data Protection Working Party which gave two purposes for acquiring personal data; one is that any personal data collected so is processed in a fair manner after it has been lawfully collected and secondly such data should be only gathered for purposes that are legitimate,….specified …., explicit and they should be adequate but not excessive of such purposes.[50] The DPAs work on whether a biometric identification system is lawful depending on Article 6 of the Directive 95/46/EC such as a whether iris recognition is necessary for air passengers will be decided on the proportionality principle. This principle also comes forward for the balancing of interest in Article 7(f) of the Directive 95/46/EC that puts forward limitation on government power for processing personal data and that such data should not violate fundamental freedoms and should only be done for interests that are of legitimate concerns such as to counter terrorism, healthcare, government IDs and others and also the extent of biometric that will be taken. For example, iris recognition cannot be

[49] Directive 95/46/EC of THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, 1995, Article 6.1 (d)

[50] Directive 95/46/EC of THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, 1995, Article 6

taken for simply making a metro card while iris recognition maybe necessary for military documents." The law was coming at the end of its validity in 2018

General Data Protection Law 2018

The "GRPR" or General Data Protection Law has one of the greatest impacts on Biometric Laws in the European Union and also internationally. It is considered the most ideal data privacy and protection law. The main focal point of the law is the principles of accountability for data privacy and data protection which is provided in the "GRPR".

The "GRPR" defines '"Biometric Data"' as personal data which results from the specific technical processing of physical, behavioural, physiological characteristics of an individual which is used to confirm the unique identification of that individual and authenticate his/her ID.[51] Art 5 (1) –(2) of the "GRPR" provides for the principles relating to the processing of the personal data. The Act provides that personal data should processed in manner that is transparent, lawful and fair emulating the principle of lawfulness, fairness and transparency. It also says that any "Biometric Data" collected must follow the principle of legitimacy; meaning that the data collected must be used for a specific, explicit and legitimate and legal purpose and the data so collected must only be processed in a manner that is suited for that purpose.[52] The next principle is the principle of data minimisation; meaning that the data collected would only be limited to relevant and adequate data which is necessary for the purpose which data is to be collected. For illustration.- In an organisation or business workplace to record the attendance of the employees only fingerprints or thumbprints are the "Biometric Identifiers" or data that needs to be collected through biometric machines by the organisation to ensure a record. That is the

[51] General Data Protection Regulation, 2018, Art 4 (14) , Regulation (EU) 2016/679, 2018 (EU)
Note- '"Biometric Data"' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

[52] General Data Protection Regulation, 2018, Art 5(1) (b), Regulation (EU) 2016/679, 2018 (EU)
Note- Art 5 (1) (b) - collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

minimal data necessary needed for the purpose of recording attendance of employees. However, if the organisation also wants DNA or voice recognition just for the purpose of recording attendance, such action is in excess and hence against the "GRPR". The fourth principle is the principle of Accuracy; meaning the "Biometric Data" should be accurate without error i.e., there should not be technological errors that fudges the data or there should not be mismatch of profile. It must also be kept up to date by erasing inaccurate data and rectifying it so it matches with the current biological or physical or behavioural or physiological profile of the individual. One of the most important principles is the "Right to be Forgotten'' meaning that "Biometric Identifiers" used for identification of a person must have a retention period and when the data is no longer necessary for the purpose for which it was procured the data must be erased.[53] The principle of confidentiality and security states that the data must be processed or handled in a manner that ensures appropriate security against unauthorised use, damage, misuse, destruction by using appropriate measures. And lastly, the law makes the controller of the data is responsible and accountable for complying with Art 5 (1) of "GRPR". Art 6 provides that processing of "Biometric Data" will only be lawful if the individual has given consent to process their "Biometric Data", or if such processing of data is necessary to fulfil a contract which the individual is a party to or if the processing of such "Biometric Data" of the individual is done in nature with the legal compliance to some law; or it is done to protect vital interests of an individual or if such processing is necessary for a task carried out in public interest. A lawful data processing can be done for the interests of the third party only if it does not violate the fundamental rights and freedom of the person whose data is to be processed.

[53] General Data Protection Regulation, 2018, Art 5(1) (e), Regulation (EU) 2016/679, 2018 (EU)
Note- Art 5 (1) (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

One of the most important aspects of "GRPR" is that it provides for the rights of the data subject in Chapter 3. The individual whose "Biometric Data" is processed shall have the right to ask from the controller whether their data is processed, if processed the purpose of such processing and the categories under which such data was processed. He has also the right to ask the controller who is the recipient of such data and especially if such data will be disclosed internationally and till which period such personal data will be retained by the other party. Also, if the data is not directly collected from the individual he has the right to ask from what source his personal data was collected and if such personal data is transferred to other nations he has the right to be made aware of the safeguards provided by the law. One of the biggest rights that an individual has is that he can ask the controller of data to provide him with a copy of the data undergoing processing. Also, any transfer of data must be notified to the individual whose data is to be transferred.

The "GRPR" also provides the Right of Rectification and Erasure of Data from Art 16-20 of the Act. The Act provides that the individual has the right to obtain from the controller any inaccurate data and rectify such inaccurate "Biometric Data".[54] As stated before one of the most important right given by "GRPR" is the 'right to be forgotten' meaning that an individual has the right to erasure his "Biometric Data" if the purpose for which it was collected is finished and the data is no longer necessary or if the data has been unlawfully processed or if the data subject withdraws consent.[55] We can see that the "GRPR" has exhaustive set of laws for data protection and privacy.

"We also see prescribed guidelines by the United Nations in its report 'United Nations Compendium of Recommended Practices for the Responsible Use and Sharing of Biometrics in Counter-Terrorism'. The compendium deals with the issues of "Biometric Data" violating data privacy and human rights and states that under the ICCPR article 17- a person cannot be subjected to any unlawful

[54] General Data Protection Regulation, 2018, Art 16, Regulation (EU) 2016/679, 2018 (EU)

[55] General Data Protection Regulation, 2018, Art 17, Regulation (EU) 2016/679, 2018 (EU)

intervention of his/her privacy and he/should have protection of law against attacks on his/her privacy[56] and the UNHRC also recognised that if right to privacy is violated or abused it affects the human rights and fundamental freedoms of persons.[57] Since, right to privacy by States must be done accordingly on the foundation of law and under very reasonable situations,[58] the compendium suggested that States should try and review their data protection and privacy laws regarding personal data so as to prevent misuse of "Biometric Data" and to meet the current standards of "Biometric Data" technologies. It also suggested for the building of procedural safeguards and the establishment of human rights approach based independent committees or bodies that will supervise the States in their use of "Biometric Data" and ensure their and the private sector's compliance of data protection and privacy laws, along with providing remedies to the victims of such violations.[59] The compendium sets forward standards that will help in establishing a biometric system compliant with laws that protect data and protect data privacy and security. The compendium set forward that the 'Enrolment Quality Assurance'[60] is a factor in setting up the system and nations should use excellent and superior quality enrolment standards to ensure accuracy even in remotest, busiest, fastest of areas and should be able to consider mitigating factors such as age of children and old person whose biometrics may show difference as they age. It also put forwards the requirement that "Biometric Data" must only be collected through informed consent through the method mentioned and only used for the stated purposes with the people having the right to correct any inaccuracy or misleading records or changing records.[61] The compendium also states that when any nation make any law or use personal data, the standards of such data should be in

[56]The International Covenant on Civil and Political Rights (ICCPR), United Nations General Assembly Resolution 2200A (XXI), Article 17, 1966
[57] Human Rights Council Resolution A/HRC/RES/34/7 (2017).
[58] Human Rights Committee General Comment No. 16: Article 17 (Right to privacy), para 3-4.
[59] United Nations Compendium of recommended practices for the responsible use and sharing of biometrics in counter-terrorism, 2018, United Nations Office of Counter -Terrorism (UNOCT), Counter-Terrorism Committee Executive Directorate (CTED), Biometrics Institute
[60] *Id.* at ,
[61] *Id.* at

conventionality with standards set by international organisations such as the International Civil Aviation Organisation (ICAO), World Customs Organisation and mainly the International Organisation for Standards (ISO) and for the purposes of protection of privacy of data the 'Privacy Guidelines and Privacy Impact Assessment Checklist' by Biometric Institute must be followed.[62] Also data should only be shared with trusted recipients and there should be prevention of misuse of personal data. As we can see from the above, "Biometric Data" should only be used for lawful purposes and must be collected legally with informed consent for a stated purpose and must not be shared without consent and that it must not be used for profit. The main principles are the following of principle of proportionality, accountability , consent of the person whose data is processed, limitation of powers of government and other data processors, transparency, ability to withdraw consent, principle of 'right to be forgotten', and others.''

Since 2018 there have been many changes on the forum of "Biometric Data" laws. At first, there was the enactment of Data Protection Law Enforcement Directive by European Union to tackle with personal data security. In 2019, along with introduction of 'Identity Service Matching Bill by Australia in July, The International Red Cross Committee adopted a biometric policy in August and Kenya also passed the Huduma Namba Bill legally authorizing the NMIMS Project. However, 2019 also saw Jamaican Supreme Court saying that the biometric ID system is unconstitutional, with three places in USA, San Francisco, Oakland and Somerville banning use of technology that uses facial recognition; however the UK High Court in the case of police collecting and using facial recognition live on people found that there was such provisions in the common law.[63] The United States of America proposed a new act in the year 2020 to regulate data privacy of biometrics through the 'National Biometric

[62] *Id.* at

[63]. AMBA KAK, ed., REGULATING BIOMETRICS: GLOBAL APPROACHES AND URGENT QUESTIONS,42 (Al Now Institute, 2020), https://ainowinstitute.org/regulatingbiometrics.html

Privacy Act' while many states in the USA introduced moratorium bills on "Biometric Data". Even in Kenya its High Court suspended the NMIMS project. Gradually we see that people became aware of the issues and risks regarding biometrics and are cautious of use of biometrics and seek to limit the power of its usage. The issues and risks of using biometrics in India will be discussed later after we discuss the present scenario of "Biometric Data" system in India.

3.3 Regulations and Legal Framework In India

The present regulation which governs "Biometric Data" usage in India is the IT Act of 2000[64] and the 'Privacy Rules'[65]. The Rules defines 'biometrics' as the technologies which measure the human body physical characteristics such as 'voice patterns' , 'fingerprints', 'facial patterns', 'eye retinas and irises' , hand measurements and DNA for the purpose of authenticating the identity of a natural person.[66] It also characterises such data under "sensitive personal data" or information.[67] The Privacy Rules provides for the collection, retention transfer and disclosure of sensitive information. It provides in Section 4 of the Rules that anybody corporate must provide for a very clear privacy policy regarding the handling of sensitive data that details the information on type of data that has been collected and the purpose for which it has been collected and that policy must be published on the body corporate's website and give the view of a clear statement of the practices and policies of the company or entity.[68] The rules provide that consent must be taken from the person whose "Biometric Data" is to be used in writing and that such information can only be used for necessary, lawful purposes and the onus is on the body corporate to make the person aware that his data is being used and

[64] The Information Technology Act, 2000, Act no 21 of 2000
[65] Information Technology (Reasonable security practices and procedures and "sensitive personal data" or information) Rules, 2011, India
[66] Information Technology (Reasonable security practices and procedures and "sensitive personal data" or information) Rules, 2011, §2 clause b, 2011 (India)
[67] Information Technology (Reasonable security practices and procedures and "sensitive personal data" or information) Rules, 2011, § 3 sub-clauses vi, 2011 (India)
[68] Information Technology (Reasonable security practices and procedures and "sensitive personal data" or information) Rules, 2011, § 4, 2011 (India)

collected for the stated person and who are the identifiers and retainers of his data and their particulars.[69] The institution or organisation is also only allowed to retain data for an amount of time as is necessary for the purpose which such data is required and it must require permission of the owner before sharing or transferring "Biometric Data" with others except for government agencies who will seek such data by clearly stating the purpose of seeking the "Biometric Data" of a person.[70] The Rules also provide for reasonable security practices and procedures in Section 8 of the Rules of 2011.

The Personal Data Protection Bill 2019 is a piece of legislation that has been inspired by the "GRPR" of the European Union and it also imports elements of the landmark judgment of 'Justice K.S. Puttaswamy (Retd.) & Anr v Union of India & Ors'.[71] It also deals with "Biometric Data" under sensitive data same as the Privacy Rules of 2011. The Bill seeks to regulate the processing of personal and sensitive data. Chapter II provides for the obligations of a data fiduciary or a person who will collect and process data. It provides that personal data must only be processed for lawful purpose and such personal data will lone be composed to the necessary extent with notice being given to the data principal – i.e., person whose data is to be collected which will encompass certain information- purpose for collection and process, what kind of data is being collected, right of principal to withdraw the consent given to process such data and the process for withdrawal, details of data fiduciaries and other entities with whom the data may be shared, his rights under the Bill and other information provided under Section 7 of the Bill.[72] The bill also provides that there will be time limit to the retention of data and data can only be retained for a necessary period to

[69] Sec 5 (Information Technology (Reasonable security practices and procedures and "sensitive personal data" or information) Rules, 2011, § 5, 2011 (India)
[70] Information Technology (Reasonable security practices and procedures and "sensitive personal data" or information) Rules, 2011, § 6 clause 1, 2011 (India)
[71] Justice K.S. Puttaswamy (Retd.) & Anr v Union of India & Ors ,2019 1 SCC 1
[72] Personal Data Protection Bill, 2019, § 7, Bill no 373 of 2019, (India)

satisfy the purpose for which the data was obtained.[73] The Bill also provides for the Rights of person whose data is obtained in Chapter V and the rights are of access to the personal data and confirmation of it, also correction of such data in case there is mistake and erasure of such data, ability access such data given to the fiduciary in course of use of services and others. The Bill offers for consent of the person before obtaining any "Biometric Data", especially that of the children. The Personal Data Protection Bill, 2019 also provides for measures regarding transparency of privacy policies and lay down guidelines on processing of data, maintaining of records, assessment of data protection impact, maintain transparency in their processing of "Biometric Data", allow for withdrawal of consent, protect data and prevent misuse and others. The Bill also provides for periodic analysis of the safeguards issued by a data fiduciary. One of the biggest and important contribution of this Bill is the establishment 'Data Protection Authority of India' under Chapter IX of the Bill, providing for redressal for breach of privacy and security of data. In case of "Biometric Data" the most important element in the above piece of rule is that of consent which is that to collect, process, share, transfer or do anything with the biometric or personal data of a person, he must be able to give clear and free consent that is not unambiguous with him being informed of the purpose and all other necessities and particulars regarding how his data will be used, processed , shared or anyway managed.[74]The personal data so collected must not be used in excessive i.e., it must follow the principle of proportionality. The Bill also provided that consent for personal data can be withdrawn. The exceptions to consent on "Biometric Data" are any Government action,

[73] Personal Data Protection Bill, 2019, § 9 Bill no 373 of 2019, (India)
[74] Suneeth Katarki , Namita Viswanath and Ivana Chatterjee, *The Personal Data Protection Bill, 2018 - Key Features And Implications*, INDUSLAW, (15 August 2018), https://www.mondaq.com/india/data-protection/727550/the-personal-data-protection-bill-2018--key-features-and-implications (July 22, 2021)

court action, action done to comply with legal order, emergency action or to an extent certain employee related action.[75]

[75] Personal Data Protection Bill, 2019, Chapter III Bill no 373 of 2019(India)

CHAPTER 4

CRITCAL STUDY ON DATA PRIVACY LAWS RELATING TO BIOMETRIC AUTHENTICATION IN BUSINESS TRANSACTIONS AND WORKPLACE.

Business sectors and workplaces use “Biometric Identifiers” for authentication of their employees and clients and partners for various purposes. In workplaces likes colleges, Institutions, offices, company offices, firms, banks and jewellery stores, and others use of biometrics to authenticate the identity of the employee and people working there is very common place. Depending on the purpose and necessity of such “Biometric Identifiers” , various workplaces or organisations buy machines from the markets for authentication purpose or even customise biometric machines. Even in business transactions or commercial transactions like payment apps or e-contracts or selling and buying with suppliers “Biometric Data” is either stored in the apps of computer systems or mobiles. For e.g., an investor wants to buy some shares of a company A, he opens a broker app that enables him to trade in shares, stocks and others. He then selects the shares he wants to buy and for authenticating his identity he uses his fingerprint from mobile or computer and then as his account details will be already within his profile in the app, the investor can with the press of fingerprint buy the shares and finish the business transaction. The world has developed a lot regarding biometrics and now our “Biometric Identifiers” are linked with our bank accounts, identity cards that has our personal information like address, age, blood group and many other personal details. “Biometric Data” is extremely sensitive and personal and should be carefully handled and one it is misused or there is unauthorised use of such “Biometric Data” it could lead to the violation of fundamental rights of a person. Also, such violations would completely infringe the privacy of a person. In India, the problem is more pronounced because the citizens have been asked by the Government to make AADHAR card where the central database has our “Biometric Identifiers” of our faces, fingerprints and iris scan. The case is grave because to avail government

schemes, for many official documents, for opening accounts or taking admissions we need to link our Aadhar card to PAN Card or bank account or produce our Aadhar Card. Now, with institutions or workplaces having our "Biometric Profiles" and even in use of fingerprint for business transactions we run the risk of unauthorised use of our data or profiling and access to our personal data by third parties or people to whom we have not given consent to have our personal data. Hence we need to critically study data privacy related to biometrics.

Data Privacy is very different from data security. Data Privacy is concerned with the handling of data like confidential data, financial data, sensitive personal data in a proper manner and to meet the requirements regarding concerned legislations. It also means protecting the confidentiality and fixity of data. The purview of Data privacy includes legislations, global variations or laws or standards, best practices, third party and governance of data. Right to privacy has been pronounced has a fundamental right in the Justice Puttaswamy judgement and privacy of one's personal data falls under the purview of right to privacy. Hence, there is a need of a comprehensive and robust legislation on Data Privacy especially relating to Biometric Data so that due to lack of laws and provisions the individuals would not suffer harm like violation of his privacy or fundamental rights and other rights. Hence, we do an analysis and critical study of the present data privacy laws in relation to biometric data especially relating to its use in workplaces and business transactions considering the increased use of such data and biometric systems in those sectors.

4.1 Data Privacy and Consent:

One of the major principles of collecting "Biometric Identifiers" to make a profile for a person is consent of the individual in collection of such data. We have seen in earlier chapter as how "GRPR", BIPA, CUBI, CCPA and other laws provided for the consent of individual in collecting "Biometric Data". Biometric Information is considered to be "sensitive personal data" or information by the "Information Technology ((Reasonable security practices and procedures and "sensitive personal

data" or information) Rules, 2011. We will only be sparsely discussing Personal Data Protection Bill, 2019 as it has yet to be enacted.

In the matter of consent for collecting "Biometric Data", the above rules provides that anybody corporate or any person on its behalf must get a written consent whether through letter or Fax or email form the individual or person who will provide "sensitive personal data" or personal information regarding the purpose of collecting such data. [76] The Rules also provide that a body corporate will only collect sensitive data and information of a natural person for legitimate or legal purpose that is related to the body corporation's functions or any activity and only if such data is considered necessary for that purpose.[77] Here the body corporate is a company or a firm or sole proprietorship store or any association of individuals engaged in either commercial or professional activities. According to the rules before collecting "Biometric Data" of a person for any purpose, a written consent through letter or email or fax is necessary. However, it is normally seen that the reality is something else. In workplaces, where "Biometric Data" is used for authentication most employees are not made aware of the purpose of collection of biometric and instead of written consent it is many a times implied consent. Firstly, in case of organisations or workplaces that use the simple fingerprint as "Biometric Identifiers" for authentication for attendance, more often than not the people are notified through the notice board as to the new office

[76] Information Technology (Reasonable security practices and procedures and "sensitive personal data" or information) Rules, 2011, Rule 5(1) (India)
Note- Rule 5 (1) Body corporate or any person on its behalf shall
obtain consent in writing through letter or Fax or email from the provider of the sensitive
personal data or information regarding purpose of usage before collection of such
information.

[77] Information Technology (Reasonable security practices and procedures and "sensitive personal data" or information) Rules, 2011, Rule 5(2) (India)

Note- Rule 5 (2)- (2) Body corporate or any person on its behalf shall not collect "sensitive personal data" or information unless —
(a) the information is collected for a lawful purpose connected with a function or activity of the body corporate or any person on its behalf; and
(b) the collection of the "sensitive personal data" or information is considered necessary for that purpose.

policy of scanning fingerprint as attendance and after the implementation of the new policy and the biometric machine, the people start providing their attendance through biometric attendance system. Nowhere their consent is expressly taken in writing through letter or fax or mail, where they are informed of all the details. One can say that since either they have contract of employment with the workplace or letter of appointment with the workplace they have to obey the rules of the organisation. However, the question here arises that if the contract does not specifically mention collection of "Biometric Data" or the appointment letter does not have any reference to collection of "Biometric Data", just that the employee has to follow all the policies and rules of the body corporate, does such contract or letter of appointment count as written consent. However, since Rule 5 (1) of the IT Rules, 2011 specifically mentions that they must obtain consent in writing regarding purpose of usage before collection of "Biometric Data", it can be simply deduced that a contract of employment or letter of appointment unless it contains specific clauses or reference to such purpose of biometric collection it cannot be considered a written consent. Same is the case for business workplaces where high level of ""Biometric Profiles" is scanned to identify the relevant person or authority and allow access to confidential documents, work, space or research or any other company or store related matters. Sometimes, some people are not even given contract or letter of appointment. It is very common in mid-level jewellery stores, department stores, and others. For illustration one of the trusted aides or employee in a jewellery store is given access to the safe or room where jewellery or precious stone is stored or we can even talk about employees who work there and use fingerprint identifier system to mark attendance. Most of them do not have contract of employment or appointment letter and although they will be informed about the purpose for which their biometrics are collected, most of the time signed or written consent is not given. Also, the definition of body corporate misses a lot of other

organisations that may collect “Biometric Data” such as NGO’s , non-for-profit organisations, organisations that are creative spaces or libraries or charity foundations as they are neither company nor firm nor store nor any association pursing professional activities but most of them are workplaces or spaces that still use “Biometric Data”. Many such organisations nowadays use biometric authentication in everyday life to either authenticate the identity of the employee or to provide access to confidential files or access to machines or simply to mark attendance. These organisations do not come under the purview of the “IT Rules, 2011” under the term of body corporate. However, since these organisations also collect “Biometric Data” it is therefore extremely necessary that the way they handle “Biometric Data” is legal and the collection of such data is done only after informed consent. Also, it is unclear as to whether the “IT Rules, 2011” covers contract or appointment letter as written consent. Also, in most commercial transactions or business transactions most of them are done through mobile payment systems or computer systems or apps. In such cases, instead of letter or email or Fax most of the time there is click-wrap agreement that either contains a contract with data privacy policy that specifies their “Biometric Data” privacy policy or they only have general data policy. It can be clearly seen that in such cases there is no written consent or agreement except for a click-wrap agreement and as such it does not fall under the purview of the above rule. As we can see that there are a lot of lacunas or loopholes in the above rules. It is necessary to form a comprehensive data privacy rule regarding consent in collection of data especially for collection of “Biometric Data” for authentication purposes in business transactions and workplaces.

The “IT Rules, 2011” also provides for withdrawal of consent. A body corporate is asked to provide the option to an individual to opt out in providing the information or “Biometric Data” to be collected. The Rules also provide that the information provider may at any time from the body

corporate withdraw his consent to collect or use his "Biometric Data". It says that such withdrawal should be intimated in writing to the concerned corporation and the corporation would then have the option to stop providing goods or services for which the "Biometric Data" was sought.[78] Here the Rules provides for the withdrawal of consent by the individual person or the information provider on the further use of "Biometric Data". However, in many cases of workplaces withdrawing of consent to the usage "Biometric Data" or biometric authentication means that the person will no longer be qualified to hold that post or work at that workplace and such many are left with option. While in paper it is a nice rule but in reality, truly employees, workers and people have no true option of withdrawing consent to the usage of their "Biometric Data" by the company or workplace if they do not want be without a job.

Another important Rule that provides for the transfer of information by the body corporate especially "Biometric Data" or profile of a person to any third party in India or anywhere in the world provided that the person or third party to whom such data is transferred adheres to a similar level of data protection as the body corporate does under IT Rules,2011. The transfer is only allowed if it is extremely necessary for the fulfilment of a legitimate contract between the company or firm and the individual or a place where the person has consented to transfer such sensitive data.[79]

---

[78] Information Technology (Reasonable security practices and procedures and "sensitive personal data" or information) Rules, 2011, Rule 5(7) (India)
Note- Rule 5 (7) Body corporate or any person on its behalf shall, prior to the collection of information including "sensitive personal data" or information, provide an option to the provider of the information to not to provide the data or information sought to be collected. The provider of information shall, at any time while availing the services or otherwise, also have an option to withdraw its consent given earlier to the body corporate. Such withdrawal of the consent shall be sent in writing to the body corporate. In the case of provider of information not providing or later on withdrawing his consent, the body corporate shall have the option not to provide goods or services for which the said information was sought.

[79] Information Technology (Reasonable security practices and procedures and "sensitive personal data" or information) Rules, 2011, Rule 7 (India)
Note- Rule 7- Transfer of information.-A body corporate or any person on its behalf may transfer "sensitive personal data" or information including any information, to any other body corporate or a person in India, or located in any other country, that ensures the same level of data protection that is adhered to by the body corporate as provided for under these Rules. The transfer may be allowed only

Although, the Rules provide for consent before transfer of information to another party, it is silent on what is exactly the level of data protection or data protection laws the country or body corporate must have; because the same level as data protection laws provided by these IT Rules, 2011 does not give a clear picture on what are the exact parameters the third party must have rules regarding collection, retention, disclosure and transfer of "sensitive personal data". An important point by the above Rules is that it says the transfer may be allowed for the necessary performance of a lawful contract. However, here there is a lacuna as in "Biometric Data" collection with biometric machine, the company may have contract with the provider for operation of the machine, who in turn may have other technological contracts for performance of the biometric machine or the company may have contracts with many other corporations for joint performance of some project and as such all these companies might need the transfer of "Biometric Data" of personnel of the company for fulfilling their part of the contract. As such in this case the "Biometric Data" of person is then simply spread or collected in various organisations who then have access to extremely personal data. Also, most of these are done through either a click-wrap contract which no one has the time to read or through employment contracts that are too huge and specifies possibilities in future tense. In reality it is very unlikely that any firm or company would every time obtain consent before transferring "Biometric Data" to third parties and hence, most of the time people are ignorant that their ""Biometric Profiles" is in the hands of many people.

if it is necessary for the performance of the lawful contract between the body corporate or any person on its behalf and provider of information or where such person has consented to data transfer.

4.2. Right to Information:

The right of an individual to know about his "Biometric Data" in possession of a data controller or company and how it is used cannot be denied. The Right to Information is also one of the leading principles of data privacy in context of "Biometric Data". The "GRPR" in Chapter 3 of the law puts the right to information as the right of the data subject or as right of the individual whose information is being collected. The individual should be allowed to know what kind of data is processed regarding him and how such data is going to be processed.

The "IT Rules, 2011" provides that a person or individual whose "Biometric Data" is collected must be informed about the fact that his information is being collected and also be made aware of the purpose for which it is collected. The individual also has the right to be informed as to who are intended recipients of the biometric information along with the name and address of the company who will retain the information and the company who will collect the information.[80]

Accordingly, a person whose biometric information is being collected has the right to be informed that his data is being collected. His data cannot be collected without his consent and without informing him about the collection of such data.

When the matter is regarding "Biometric Data", it is necessary that the knowledge of the purpose of the data collected is being made known to the information provider. If, information regarding the purpose of collection is withheld than the information provider might be cheated out

[80] Information Technology (Reasonable security practices and procedures and "sensitive personal data" or information) Rules, 2011, Rule 3 (India)
Note- Rule 3- While collecting information directly from the person concerned, the body corporate or any person on its behalf snail take such steps as are, in the circumstances, reasonable to ensure that the person concerned is having the knowledge of —
(a) the fact that the information is being collected;
(b) the purpose for which the information is being collected;
(c) the intended recipients of the information; and
(d) the name and address of —
(i) the agency that is collecting the information; and
(ii) the agency that will retain the information

of his “Biometric Data” and his data may be misused. Also, the purpose for which the data is being collected must be a lawful and legitimate purpose. However, unlike the BIPA or “GRPR” the IT Rules, 2011 does not say that the purpose has to be specific and explicit. Here, there are two main problems. Firstly, that while the purpose for collection of data can be lawful, the information provided to the information provider about the purpose of the collection of data may be vague or unclear. Nowhere in the IT Rules, 2011 it is mentioned that the information of the purpose must be clearly given or completely provided. It just mentions that the purpose for which data is being collected must be informed to the person. Herein, lies the problem, if a person does not know clearly the purpose for which his “Biometric Data” is being collected, is he in a position to make correct judgment to give consent for the collection of the data. For, illustration A works in a school. He is informed that his “Biometric Data” will be collected for the purpose of school related matters. Now, as per as “IT Rules, 2011” he has been informed about the purpose for collection of his “Biometric Identifiers”. However, in the above example A is not being clearly told on what matters exactly his “Biometric Data” is collected. Secondly, unlike the “GRPR” or BIPA the purpose is not needed to be specific or explicit in nature. Taking the above example, we can see how it clearly creates a lot of problems. Here A is only told his “Biometric Data” is collected in relation to school matters but the specific purpose or reasons for which his data is collected and is to be used is not mentioned. Commonly, a person will suppose that his “Biometric Data” is used to mark his attendance as it is what is used in schools nowadays. However, school related matters may include many other purposes for which the person’s “Biometric Data” is used such as performance register, profile creation, and many other things. If such things or matters are not clearly mentioned than a person will be unaware as to for what exact purposes his “Biometric Data” is used. Also, such matter will hinder the person from giving an informed consent with clear judgment.

Hence, it is extremely necessary and right of the individual to be informed about the complete purpose for which "Biometric Data" is collected. The "IT Rules, 2011" severely lacks in that aspect.

The "IT Rules, 2011" provides that it is pertinent for an individual to know who is collecting his biometric information and their details. It provides that the individual should have the information on who are intended recipients who will receive the "Biometric Data" and the name and address of the agency who is collecting the information and the agency that will retain the information. Herein, we see three parties who will handle the biometric information of the person; one the agency or body who will collect the data, two the agency or body that will retain it and third the intended recipient of the data. Although, the Rules 2011 provides that the name and address of the agencies who collect data and the one who retains it must be provided, however it does not provide that the details of the intended recipient should also be provide, only who the body corporate is must be provided. For illustration, let's take our mobile smartphone that have fingerprint or face lock. Now here is the situation, it is the software and hardware of the device that collects the data, this data is then fed to operating system of the device who makes biometric authentication possible. Now the operating system is again another agency or body. The company who probably looks after the whole function is the parent company because the privacy policies and contract will be with them. However, it is the operating system in the device that will retain the data. Now comes the question where such data is stored whether in cloud or data centre or anywhere else. Again, except for use fingerprint to unlock our smartphones we also use fingerprints or voice recognition to interact with various apps to make purchases, write mails or do other work. Now the question comes whether the apps or devices are only the intended recipients of the "Biometric Data" or also the agencies retaining and collecting data. For example, Alexa or Siri can voice authenticate through multiple devices be it smartphones, laptops,

smart home appliances and others. In this case, it can be clearly seen that any company or operating system or software behind them is the all the three, collector, retainer and the intended recipient. Then what becomes of the device through which the information was collected, cause the operating system of such a device will retain the data as well as the company for the purpose of next authentication. As we can see, it is a chain of organisations through whose network the "Biometric Data" passes. The "IT Rules, 2011" completely ignore such complexions and only divide them into collectors, retainers of data and the intended recipient. There is no provision to provide the individual with the identity and details of all the parties who in the long complex process will come in contact with the individual's "Biometric Data". Also, while the Rules provide for disclosure of data to third party with permission of the individual, it does not provide for providing the information of details of the third parties to whom data is disclosed or transferred to the individual. We can here rightly say that the IT Rules, 2011 needs to take into consideration the complex process involved in the collection of "Biometric Data" and also all the parties concerned to make more comprehensive rules regarding information to be provided to the individual.

In processing of "Biometric Data", the "IT Rules, 2011" is silent on the right to information of the individual to have information on whether his "Biometric Data" is being processed, what categories of "Biometric Data" is being processed. Unlike "GRPR" there is neither any provision where an individual is provided with a copy of list of the "Biometric Data" undergoing processing nor any provision where the individual whose "Biometric Data" is undergoing processing can ask for it.[81] It

[81] General Data Protection Regulation, 2018, Art 15 (3) , Regulation (EU) 2016/679, 2018 (EU)
Note- Art 15 (3)- The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject; the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

hampers the freedom and the right to information of the individual to know what has been being done with his own personal data. Since, "Biometric Data" is "sensitive personal data" it is of greater concern if the provider of the data has little to no knowledge for what reason is his data being used. Apart, from the above there is no provision where the individual can ask the body corporate for the duration of period his "Biometric Data" will be retained by the body corporate. Also, nowhere any provision is provided on an individual's right to information regarding the finishing time of the purpose or project for which his "Biometric Data" was collected. The most concerning thing is that while the "IT Rules, 2011" says that the purpose of collecting must be lawful, the Rules does not provide the individual any right to ask information to the body corporate the legal basis and principle behind such collection and processing of data. A person has the complete right to seek information about his own personal data. In the case of Manohar Singh v National Thermal Power Corporation Ltd[82], it was decided by the Central Information Commission that when a citizen is seeking information about himself then as long as such information to be given is not prohibited by the Right to Information Act, then such a citizen cannot be denied any such information. Here, a person has the right to know about the processing of his "Biometric Data" done by others.

4.3 Retention of Data:

"Biometric Data" is extremely sensitive data and personal to an individual. According to Puttaswamy v Union of India , Puttaswamy I,[83] Right to Privacy is a fundamental right of an individual and such a right also encompasses right to decide who can use a person's data about physical or physiological attributes or "Biometric Data". Retaining "sensitive personal data" for a long time will affect the privacy rights of a person. The law provides that anybody corporate

[82] 2006 SCC Online CIC 684, Appeal No 80/ICPB/2006, Central Information Commission,
[83] Puttaswamy v Union of India , Puttaswamy I, Writ Petition (Civil) No. 494 of 2012,

can only retain "Biometric Data" of a person till a time that is required for the fulfilment for the purpose for which such data was collected. They can also retain data if it is required under any law that is in force for the time being.[84] Here any organisation can only retain data if its required to retain such "Biometric Data" to fulfil the lawful purpose or objective of collecting such data. It provides that no organisation can retain any data for an indefinite time. However, there are still number of issues regarding the period for which the organisation can retain data.

Firstly, the Rule does not specify nor there is any other provision on when it will be considered termination of relationship between the body corporate and the individual. It merely states that when the purpose is finished the body corporate must not retain the "Biometric Data". It does not clarify on whether the "Biometric Data" must stop being retained after the initial purpose is fulfilled or the original purpose is fulfilled or after subsequent but connected purposes are fulfilled. The above law is also silent on whether information on the period of retention of "Biometric Data" is to be intimated to the individual or not. It hampers the individual's rights when he is not made aware of any information or data regarding him being in use. Also due to non-specifying of the period needed to fulfil the purpose the individual might think that the purpose is completed so his data is no more retained in the system only to later find out that his "Biometric Data" has been retained in the system for years. Also, in the "IT Rules, 2011" we talk about body corporate and a body corporate has workers or employees. In these Rules unlike the BIPA or other rules there is no provision on when does the relationship between a body corporate and its employees is over. In BIPA after an employee either resigns from work or his work contract is over then his relationship with the body corporate is over and the body corporate no longer has the right to retain his "sensitive personal data". Also,

[84] Information Technology (Reasonable security practices and procedures and "sensitive personal data" or information) Rules, 2011, Rule 5 (4) (India)
Note- Rule (5) (4)- Body corporate or any person on its behalf holding "sensitive personal data" or information shall not retain that information for longer than is required for the purposes for which the information may lawfully be used or is otherwise required under any other law for the time being in force

they must no later than 3 years after an employee leaves work must delete his "sensitive personal data" like biometrics. Indian law is silent on such matters and the scope of the law in "IT Rules, 2011" is much narrower. Also, the above law does not address the retention of "Biometric Data" collected by body corporates through mobile apps, laptops or through machines that is used to access certain services. When we use mobile apps to do business transactions and use biometric authentication, the data is integrated into the data base. However, when we uninstall the apps the "Biometric Data" is still being retained. Hence, again when we install the same app we can operate the app with "Biometric Data" and authenticate our identity. Most apps do not even have the option to delete our account and thus they can retain the data for ever. It is necessary to make certain laws or rules so that apps that use "sensitive personal data", especially "Biometric Data" if a user is inactive for a period of years will notify the user about it and the retention of "Biometric Data" by the app and also provide an option to the user to continue using the services or if the user does not want to continue the app should no longer retain the "Biometric Data". It should be the same case for other biometric machines.

The second issue is that the "IT Rules, 2011" says that the body corporate can retain "sensitive personal data" if a law that is for the time being under force requires it. It means that if there is any and it means any law that requires a body corporate to retain "Biometric Data" of a person they have to retain it. They can also make the body corporate under law to retain the data permanently. So basically, the purpose of the above rule prescribing a limited period of retention in the face of such laws becomes worthless. Also, the objective to retain and collect data only for the purpose that is informed to the individual becomes void, cause the laws that are being in force will surely have different purpose than that of which the "Biometric Data" at the initial stance was collected. Such retention could lead to gross violation of fundamental rights. If the government makes laws that allows intelligence agencies or bureaus along with law enforcement and other government agencies to collect "Biometric Data" from organisations and use it for profiling of a person than it will hamper the right to privacy of the

individual. Unlike in other countries' biometric laws which have laws against use of "Biometric Data" for profiling except for certain circumstance India does not have such laws. Hence, to prevent violation of fundamental rights and right to privacy of an individual there must be a balance between the individual interest and rights and the government interest. There must also be clear specifications for what purpose and for how long of a period "Biometric Data" can be retained.

4.4 Right to be Forgotten:

In the above point we talked about retention of data and that a body corporate can only retain the "sensitive personal data" till the purpose for which "Biometric Data" is procured is fulfilled except if required by law. However, the "IT Rules, 2011" do not provide as to what happens to the data after that and how such data is to be disposed. It is completely silent on that matter. Not only we do not have a rule or law regarding the disposing of such data, we also do not have any law through which a person can ask for disposal of such data. "Biometric Data" is a person's personal data and is extremely sensitive in nature and hence long retention or inappropriate use or disposal of such data is violative of his Right to Privacy and human rights . A person should have the right to be forgotten in a database. He should be able to ask for permanent deletion or erasure of his data.

One of the most important principles involving "Biometric Data" and Data Privacy is the principle of the "Right to be Forgotten". This principle means that a person has the right to get his "sensitive personal data" erased from a database, provided that such data is still not needed for any legitimate purpose i.e., the initial purpose for which such data was necessary. There can be no lifetime record of any "sensitive personal data" especially "Biometric Data". The principle of "right to be forgotten'' has been provided in many biometric laws such as the "GRPR", BIPA, "United Nations compendium on the use of Biometrics for counter-terrorism" and others. It is one of the pivotal principles

that ensures the right to privacy of the individuals and ensures data privacy of "sensitive personal data".

The principle of "right to be forgotten" provides that a data subject or individual who provides his "biometric data" to any entity or government or organisation or anyone else has the right to ask the data controller to completely and permanently erase his biometric profile and identifiers from all the databases or any particular database. [85] The data controller has the obligation to erase the data without any undue delay if the purpose for which the data was collected is fulfilled; if there is withdrawal of consent by the individual; if the individual is objecting to the processing of his biometric data ; if for some reason the "biometric data" is wrongfully processed by any of the parties and if by any legal obligation the controller is required to erase such data. The controller must take steps to inform other data controllers that the individual has requested erasure of data if he has either shared the data with consent or has made the data public pursuant to some order. He can then however only erase such data if it is not against any law.

Indian data privacy laws are much narrower in nature and does not provide for the principle of "right to be forgotten". The Personal Data Protection Bill, 2019 although puts forward a token provision in the name of the principle of "Right to be Forgotten"; however, erasure of biometric data of an individual unlike the main principle and provision of other countries is not a matter of right but is subject to the approval of the Adjudicating Officer.

4.5 Data Privacy and Data Collection Limitation:

The "IT Rules, 2011" provides that only such "sensitive personal data" will be collected by a body corporate if it is collected for a lawful purpose and is related to any function of the body corporate and is necessary for the fulfilment of

[85] General Data Protection Regulation, 2018, Art 17 (1) , Regulation (EU) 2016/679, 2018 (EU)
Note- Art 17 (1)- The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:
(a) ……

purpose for which the data was collected.[86] The Personal Data Protection Bill provides for collection limitation meaning that it limits the collection of sensitive personal data to the data that is necessary for the purposes of processing.[87] It means that any organisation or entity or government or any individual can only collect such amount of data as is necessary for completing or fulfilling the purpose for which data is collected. Now, the question is who decides what is the necessary amount of biometric data needed for the project. Is it the law, the government or the entities? Both above laws are silent on that, the only criteria that is given is that it must be necessary for the purpose. Well, even voice recognition can be made necessary for a purpose. There are no particular standards which prescribe the type of biometric data to be used for fulfilment of a purpose. Herein, comes the principle of data minimisation that is given by the GDPR. Data minimisation means that data should not be collected in excess, it must be collected taking in consideration the purpose the data is going to be used. For illustration. A person X works at a college and for attendance he needs to authenticate and verify his biometric data. The most minimum technology necessary required for such an activity is a biometric fingerprint punching machine which will help record the attendance. It is not necessary to collect "biometric identifiers" like iris recognition or voice recognition just to mark attendance. However, for access to computers that contain data of main accounts of a business and confidential document, fingerprint scan, along with iris scan along with face scan and voice recognition may be necessary. So, depending upon the purpose there is necessity of identifiers that need to be collected. Data minimisation means collecting only

[86] Information Technology (Reasonable security practices and procedures and "sensitive personal data" or information) Rules, 2011, Rule 5(2) (India)
Note- Rule 5 (2)- (2) Body corporate or any person on its behalf shall not collect "sensitive personal data" or information unless —
(a) the information is collected for a lawful purpose connected with a function or activity of the body corporate or any person on its behalf; and
(b) the collection of the "sensitive personal data" or information is considered necessary for that purpose.

[87] Personal Data Protection Bill, 2019, § 6, Bill no 373 of 2019, (India)
Note- Section 6 - Collection limitation. —Collection of personal data shall be limited to such data that is necessary for the purposes of processing.

the most minimum necessary data that will get the task done. There is no point in collecting biometric identifiers such as iris scan for only simple attendance. However, such limitation in collecting data has not been clearly provided in Indian laws and no standard has been set. Businesses or organisations may overstep their limits in collecting all kinds of biometric data from a person even if it is not exactly necessary for the purpose as the standard of what consists as "necessary data" has not been set. There needs to be a law to limit the powers of businesses or organisations.

4.6. Data Quality and Accuracy:

"Biometric Data" is personal data that is derived from the physical, behavioural and physiological characteristics of a person. Identifiers are things like face recognition, fingerprint scan, voice recognition, and others. Such physical attributes with age face wear and tear and even changes. A fingerprint of a person might change because of some injury, faces always changes as persons grow older. Biometric Data of a person is used for verification, identification and authentication purposes. So, when the physical or biological characteristics of an individual changes over time it will be very difficult to verify or authenticate the identity of someone with the old biometric data. It will also stop the individual from access to services or privileges that he was enjoying. Hence, it is important to periodically review the biometric data of an individual. Also, biometric data should be correct and accurate, meaning that the data collected should be such that it matches the biological characteristics of the individual and is collected without any technological defects or others. For illustration. A has provided thumbprints of both hands as biometric identifiers. A's left hand thumb print should be marked as such in database and right-hand thumb print as right-hand thumb print. The right-hand thumb print cannot be marked as left-hand thumb print in the database, if it is done so the data will be inaccurate and incorrect.

Workplaces and business transactions deals with the biometric data of a large number of individuals. Every authentication or verification provides access to

different things and affects the daily working capacity. So, if a data is not accurate and correct it would really cause a lot of issues. Both the IT Rules 2011 and the "Personal Data Protection Bill" provides that the sensitive personal data should be complete, accurate, correct and most importantly updated. [88]The data should be periodically reviewed and if any incorrections or inaccuracies are found then they should be corrected.[89] Also, it must be a policy to review data periodically by all the organisations and businesses so that such inaccurate data can be corrected. The individuals must have the right to review any biometric information they have provided and periodically have them either updated or any inaccuracies corrected and amended as soon as possible per the laws.

4.7 Processing of Biometric Data:

It is very important any processing of biometric data is lawful, fair and transparent to ensure that such data is not misused or there is no unauthorised use or access to such data.[90] Fair and transparent processing will allow the data principal or individual know as to which categories of his biometric data is being processed, who is processing such data, who will receive such data and the data

---

[88] Personal Data Protection Bill, 2019, § 9, Bill no 373 of 2019, (India)
Note- Section 9 – Data Quality . —. Data quality.—
(1) The data fiduciary shall take reasonable steps to ensure that personal data processed is complete, accurate, not misleading and updated, having regard to the purposes for which it is processed.
(2) In considering whether any reasonable step is necessary under sub-section (1), the data fiduciary shall have regard to whether the personal data—
(a) is likely to be used to make a decision about the data principal;
(b) is likely to be disclosed to other individuals or entities including other data fiduciaries or processors; or
(c) is kept in a form that distinguishes personal data based on facts from personal data based on opinions or personal assessments.
(3) Where personal data is disclosed to other individuals or entities, including other data fiduciaries or processors, and the data fiduciary subsequently finds that such data does not comply with sub-section (1), the data fiduciary shall take reasonable steps to notify such individuals or entities of this fact.

[89] Information Technology (Reasonable security practices and procedures and "sensitive personal data" or information) Rules, 2011, Rule 5(6) (India)
Note- Rule 5 (6)— Body corporate or any person on its behalf permit the providers of information, as and when requested by them, to review the information they had provided and ensure that any personal information or sensitive personal data or information found to be inaccurate or deficient shall be corrected or amended as feasible:
…….

[90] Personal Data Protection Bill, 2019, § 4, Bill no 373 of 2019, (India)

is being processed for which purpose. Also, the biometric data must be processed in a way that respects the right to privacy of the individual, meaning the data must be kept secure without breaches and confidential and only to the parties who are allowed to access such data.

Biometric Data of employees, clients, partners, workers and customers are an asset to any Business or organisation. When the law says that there must be lawful and fair processing of biometric data, it means that every procedure given by law must be followed and it must be fair. Consent is one of the pivotal elements when processing biometric data. Free Consent has always been the elements of a valid contract and an organisation or business needs to obtain permission from any individual before collecting his "biometric data" such as fingerprint scan, voice sample, facial image and others for verification and authentication purposes. Before processing biometric data for workplaces or business transactions any entity doing so is required to obtain explicit consent from the individual, meaning the person must be told the purpose of processing such data and that processing of such data will have significant consequences for him; the consent must be clear and not implied and that consent must be specific in that the individual must have options for separately consenting for different purposes, different operations and different categories of biometric data.[91] Unfortunately, the above provisions are only provided in the "Personal Data Protection Bill" and this Bill is yet to be enacted. The "IT Rules 2011" does not provide with any provisions on what is considered fair and lawful processing of sensitive personal data. In the legal arena of biometric data, it is

[91] Personal Data Protection Bill, 2019, § 18 Bill no 373 of 2019, (India)
Note- Sec 18- Processing of sensitive personal data based on explicit consent. — (1) Sensitive personal data may be processed on the basis of explicit consent.
(2) For the purposes of sub-section (1), consent shall be considered explicit only if it is valid as per section 12 and is additionally:
(a) informed, having regard to whether the attention of the data principal has been drawn to purposes for operations in processing that may have significant consequences for the data principal;
(b) clear, having regard to whether it is meaningful without recourse to inference from conduct in a context; and
(c) specific, having regard to whether the data principal is given the choice of separately consenting to the purposes of, operations in, and the use of different categories of sensitive personal data relevant to processing.

very important to define and make rules on what is considered as lawful processing of such data as exemplified by "GDPR" and other biometric laws. More so ever, in reality specific and explicit and written consent does not happen. Let us take for example an app that uses biometric data. The app will contain mostly two click-wrap contracts one with terms and conditions which a person has to agree to use the app and another one a privacy policy. Both are extremely long and cumbersome and something the layman does not understand at all nor has the time to read. Also, the clauses related to biometric data will be sometimes separately spelled out in privacy policy and at other times comped together just as data and the segment will be somewhere far below in the contract. Same is the case for employment contracts. So, most of the time people do not even know what they are consenting to and is shocked later when their information is profiled or collected by other companies as means to profit.

4.8 Third Party:

One of the biggest risks in dealing with biometric data is the unauthorised sharing of sensitive personal data with third parties by the businesses or organisations. The "IT Rules, 2011" in Rule 6 provides that before disclosing any biometric data to any third party one must obtain prior permission from the individual from whom the biometric data was obtained. It also mentions that the third party must have a legal contract with organisation or business. A business or organisation can also disclose biometric data of an individual if such disclosure has been agreed to in a contract by the individual and the organisation. And herein, in reality lies the crux of the issue. The problem as stated above are the long contracts with thousands of clauses that the common layman does not understand. In paper and legal terms , we can say prior permission or consent has been obtained but in reality nothing such happens. Again, sometimes there be no mention of biometric data in privacy policy. Let's take Google for example here. In many devices we can log in to our Google Accounts through biometric authentication and even operate Google Pay with it to do Business Transactions. The Privacy Policy of Google although underlines that they will share "Sensitive

Personal Information" with explicit consent of the user, but when you click on the link to check the definition of sensitive personal information there is no mention of biometric data.[92] Now the question is whether the device is the main collector of the data and google an intended recipient of it for usage. It is not even clear as to who is the collector of the data let alone providing informed permission to share or disclose data to third parties.

Now, the second crux of the issue is when a person knows who is the initial collector of the data or the retainer of the data. In most workplaces or organisations where employees sign contracts with the employer, in the contract itself the organisation will mention about sharing data with third parties as and when required and when the worker or employee signs it, it will be agreeing to the terms. However, third parties who need disclosure of information will be many and keep on changing as and when required due to projects or collaborations taken by the organisations. However, the law does not provide for asking repeated and separate permissions every time there is a need for disclosure to third parties. Also, unlike in transfer of information to third parties, there is no assurance on which law will then govern the biometric information if the third party is some entity or organisation outside India.

4.9 Transparency:

As we talked about in the chapter relating to legal framework, one of the major principles regarding "biometric data" laws and data privacy is the "principle of transparency". This principle says that any organisation or entity who deals handles biometrics must be transparent and fair in handling and processing of such data. It is the obligation, duty and responsibility of the organisation to be transparent in all its dealings. It means that the dealings will not be done in subterfuge and every aspect will be dealt in a legal and lawful process. There should be no implied or hidden aspects or information that cannot be made

[92] With Your Consent, When Google Shares your Information, Sharing of Your Information Privacy Policy, https://policies.google.com/privacy#infosharing

available to the provider of the biometric data. It must be clear and fair and transparent.

Transparency in processing data has been provided in the "Personal Data Protection Bill"[93]. The Bill states that the individual whose data is processed or collected must be provided with the information as to the manner and content of data collected along with the purpose regarding which such data was collected. One of the important provisions in the Bill regarding transparency is that it provides information should be intimated to the individual if any categories of biometric data (personal data) is processed in exceptional purposes or situations and would carry a significant harm to the individual. The Bill also provides under the provisions of transparency, that the organisation or business must provide information regarding particulars on what are the rights of an individual providing biometric data and how can he exercise his rights. The individual should also be informed about grievance redressal authorities and of third party and cross-border transfers. Transparency in handling data protects the human rights of the individual. However, the current IT Rules, 2011 does not provide any provisions regarding it. Hence, even if workplaces or business organisations are not transparent in their dealings, or fail to provide with certain information requested by the individual except that data is collected, purpose of the data collected, name and details of the handling parties it will fail because there are not many provisions in the Rules and there is no law to enforce it. That is to say a body corporate can get away with ignoring the human rights and privacy rights of the individual.

4.10 Data Security Safeguards:

It is very necessary to prevent breach of data and maintain confidentiality and security of data. If data like biometric data is leaked it would be a huge problem for the person. People may use such Biometric Data for profiling, stalking and even committing Identity Theft. Identity theft is one of the biggest security risks

[93] Personal Data Protection Bill, 2019, § 30 Bill no 373 of 2019, (India

regarding biometric especially for those corporations, businesses or organisations that have confidential documents or valuable things or require high level professionalism or require work of specific person and others. Identity theft would completely violate the fundamental rights, human rights and privacy rights of a person. Generally, Identity Theft regarding biometric is a huge problem because biometrics are a person's biological attributes and remain with that person. Once it happens unlike PIN or Password there is no possible reset and to make the information correct it would take a long and arduous process. It is even hard to imagine what kind of evidence and proofs would be needed to set something. In India, though we presently have grievance redressal forum, we don't even have a set procedure or rules that will help restore a person's data after identity theft using biometric data is proven. For illustration Imagine B hacks into the database and replaces A's biometric identifiers with his own like fingerprints, facial image and others. How would An even begin correcting the theft when all the data systems will show B with his face living at A's address and having his qualifications or others. Here, B will become A and a will have a hard time proving that he is the real A. Now imagine in a company it happens where a high-level employee is knowledgeable about confidential things regarding the company, the whole company will be in extreme jeopardy. So, it is very necessary to have top-notch security safeguards for the security and confidentiality of biometric data.

The "IT Rules 2011" provides for "Reasonable Security Practices and Procedures" a body corporate must follow when operating with data. It provides in Rule 8 (1) that a body corporation will be said to have compiled with reasonable security procedure and practice, if they have implemented such "security practices and standards" and they must have a complete documented and comprehensive security programme and information security policies. This programme and policies must contain an in-depth information on the technical, managerial, operational and physical security measures and they must be adequate and appropriate for protecting information and data assets. In case of data breach, the body corporation is required to show that they have security

measures as per as their documented policies and measures. The Rules also state that body corporates should follow “The International Standard IS/ISO/IEC 27001 on "Information Technology - Security Techniques - Information Security Management System - Requirements" as it is one of the stellar Standards of data protection, privacy, and security. Any other best practices of data protection or Standards followed by body corporates must get the codes of best practices approved by the Central Government before implementation. The Rules also provide that the codes of best practices must get certified or audited by an independent auditor on regular basis. The Data Privacy rules provide for adequate security practices and standards, however for biometric data ISO also has certain other Standards for biometric security which are not provided by the Rules.

4.11 Privacy Policy:

A privacy policy is extremely important for an organisation or Business that uses or collects or retains biometric data. It has been repeatedly said that biometric data being sensitive data must be kept secure and confidential and there must be prevention of unauthorised use. A privacy policy is to be compulsorily provided by a body corporate handling or dealing with sensitive personal data to the person who provides such data and such a privacy policy must be made available for their view to all individuals who have provided biometric data. The Privacy Policy must be published at the body corporate’s website and must contain clearly and in an accessible manner the statements of its practices and policies and what is the type of data collected, for what purpose, about disclosure of information and the security practices and standards of the body corporate.

Currently there are a few issues with the prescribed law and reality especially in cases of business transactions and workplaces. Firstly, although the Rules of 2011 provide for the publication and making of privacy policy by the body corporate, except for a few basic essentials elements to be included it does not provide for other standards or other rules and regulations to be included. A body corporate can after including the given data make a privacy policy as they wish.

The law does not provide for the standard to be maintained in the privacy policy and the elements are included in a much narrower scope foregoing important rules to be included on consent, transparency, correction and rectification of data, third party policies, processing of data and many other elements which are extremely vital to data privacy and protection of biometric data. It in fact gives body corporate free rein to do as they wish.

Secondly, while the law mentions that privacy policy must be published in website, there are many organisations or businesses whose privacy policies either does not include specific measure or rules on biometric data or these organisations do not have a privacy policy published on the website.

The present legal framework regarding biometric data and data privacy especially in relation to workplaces and business transactions is very weak and narrower in scope. Unlike comprehensive international laws like GDPR many vital and important data privacy principles in regard to biometric data has not been provided for by the Rules. The IT Rules 2011 provides for laws or rules for the body corporate, however the definition of body corporate and many organisations which use biometric data fall outside their purview and currently there are no other laws that deal with biometric data used by businesses and organisations; not counting Aadhar Act as it provides mainly for Government related laws. Nowadays, usage of biometric data is so common in offices, companies and for e-commerce that there is need for a comprehensive legislation to address such issues. The current laws do not give clarity of purpose for which data is collected and neither it provides that purpose needs to be specified each time and informed every time. One of the biggest problems is of consent to provide biometric data and the current rules fail in taking into account issues such as explicit consent, different ways and forms of consent, consent for every time different categories of data is processed and most importantly of all as what forms as informed consent. The next biggest problem is of privacy policy as the current law does not specify many vital parameters that needs to be followed by a company or any entity that collects biometric data. Also because of that a company or organisation may not bother upon lawful,

transparent and fair processing of biometric data. Another big problem related to third party issues is data sovereignty. India historically did not have its own data centres where huge amounts of metadata or big data is stored, hence most biometric data was either stored in “Cloud” or in data centre of other countries. The present law does not clarify as to what standards such data centres are expected to follow in handling data and storing them and whether the country where such data centre is will follow or Indian laws will prevail. The present legal framework of data privacy in India fails international standards and there is need to make a comprehensive legislation. Also , the present legal legislation does not mention anything on profiting and profiling. The current legislation does not stop companies or organisations from making profit by trading, selling or buying biometric data or using it as a part of trade deal that is unfair and is geared towards taking advantage and garnering profit by obtaining such biometric data. The present legislation also allows disclosure of biometric data to the government upon asking and to any authority if it is provided by law. Government can use such data for profiling, in fact India is considered one of the countries that conducts mass surveillance using biometric data. There are no provisions that limit the power of the government. The present IT Rules need either reframing or there is basically an urgent need to bring a new legislation on biometrics if people has actually to main privacy of data.

CHAPTER 5

CONCLUSION AND SUGGESTIONS

As the year 2021 rolls by many employers are using biometric data more and more and it has become common place for the new generation to transact through mobile phones, laptops or even devices that uses biometric data to work or trade in things. For illustration, Siri and Alexa are capable of recognising voices and are able to perform many actions like even buying things from the web or writing mail or take dictation for writing a report. It is seen with the advent of new and easily affordable technologies and machines have made organisations and businesses opt for biometrics and biometric authentication. There has been the emergence of companies in India who are making biometric machines and these machines are being sold to various organisations. Nowadays, even mobile phones, laptops and others are equipped with biometric applications and facilities to authenticate biometric data. Biometric data is being used for something small as recording attendance to huge as providing access to labs. The Medical Council of India has apparently under the Digital Mission Mode Project has mandated to record the attendance of all staff and faculty of medical colleges or institutions through biometrics. Banks have apparently allowed during the Covid-19 pandemic to fill e-KYC forms and authenticate and verify their identity through video calling. We can conclude that in present times biometrics and authentication of biometrics to use services, do commercial transactions or even work in developed workplaces or organisations has become exigent and compulsory.

The International framework regarding biometrics is vast and stellar and it provides for comprehensive laws regarding data privacy. In India, at present any law that is in force regarding biometrics is the IT Rules, 2011 and the Aadhar Act,2016. The provisions of the IT Rules,2011 deal with company or body corporate however as seen the scope of the law is much narrower. Under the purview of the rules much workplaces and organisations has been left out and

there are no rules governing them. Most of the rules are grouped together with regular data and there are hardly a few rules separate for sensitive personal data. Considering, how personal and sensitive biometric data is to a person and any breach of data could end in a tragedy for a person by becoming victim to serious offences such as profiling, violation of privacy, mass -surveillance and identity theft, it is extremely surprising to see inadequate and scant provisions in the IT Rules, 2011 that are just in name but in reality are incapable of data protection. In case of identity theft there is almost nothing that anyone can do to help the victim. The rules are completely fall short in providing any security to the people. There are so many provisions that do not meet international standards and parameters that there is chance of attack or hacking resulting in violation of privacy and the fundamental rights of the individuals. Also, in this case the Aadhar Act, 2016 does not apply much as the process is a separate way of biometric authentication done within the purview of the organisation without the use of Aadhar Card. The Personal Data Protection Bill also does not apply as it has not been enacted yet. The law has a lot of lacunas upon analysis.

Consent has always been one of the most important principles of data privacy and policy. The present rules are much narrower and do not provide for informed consent. In the current scenario, when biometric data is provided to the companies or head of organisations by employees or workers as a matter of fact, it is unclear as to how many of them were in clear terms informed through any written document about the details regarding the processing of their biometric data and give informed consent. More often than not, it is taken as part and parcel of their jobs by employees and workers. Even, people who use mobile phones and various apps are unaware of what they are consenting about.

Several provisions of the IT Rules, 2011 were very much limited as well vague in their meaning and not encompassing all the parameters that is necessary to safeguard and protect data. In fact, as found in reality many of the provisions are not even applied, mainly due to lack of knowledge and even when applied the laws instead of making it simple and clear for the layman, helps the company

or organisation in making such rules and laws in their policies that end up profiting them.

The current IT Rules, 2011 although it says it provides rules for a body corporate i.e., a company or a fir or sole proprietorship in regard to handling data and data privacy, there is huge inadequacy in terms of exactly protecting data especially biometric data and keeping it secure and confidential by the virtue of the provisions of the Rules. The Rules have foregone many of the important principles in data privacy. There are no provisions describing and providing the parameters of lawful processing of data that will hold the standard and prevent from companies or workplaces from taking advantage of individuals who work with them. The provisions of the Rules do not provide for a stable and steady structure for the handling of biometric data and there are many loopholes that will allow for the breach of privacy. The Rules allow the companies to formulate their own privacy policies with providing the only bare minimum parameters of keeping the data subject informed on a few things, however it has been found that most privacy policies either include only vague clauses on biometric data separately or in some cases not at all.

In India, there is no adequate laws on biometric data in terms of data privacy. The current laws do not protect the data principal's data from government snooping or surveillance. It also does not protect the data principal from third party issues as the present laws are not stringent on the provisions allowing sharing of data with third party. One of the major concerns is that the unawareness of many laymen who use biometric data for authentication purposes in workplaces or everyday lives of their rights as data subject, the right to get information and even that there should have been explicit and written consent on their part before the company used their biometric data. The current laws have failed in providing assurance on protecting data privacy of biometric data with important parameters such as principle of transparency and fair processing, failure to set up redressal mechanism when there is security breach or identity theft or others and of procedures of restoring the identity and correcting the harm, failure to provide the right to erase data permanently, failure

to set up an ideal standard for privacy policy and provide stellar parameters and standards being absent from the present laws. Even the current provisions in many ways are very much narrower in scope and does not take into consideration the complexities of handling biometric data. The current legislation is neither comprehensive nor effective in dealing with the complexities provided in handling biometric data and ensuring data privacy. In fact, the present situation regarding usage of biometric data in workplaces and business transactions is that there is no awareness as to which laws apply to the situation and the companies are using the huge loopholes in the law to in fact use the law for their own profit. They are complying with the laws on mere paper. Hence, there is threat to the data privacy of biometric data of employees, workers or customers and there is necessity of new comprehensive legislation to ensure strong data protection and privacy and ensure the fundamental rights are not breached, along with providing for smooth operation of biometric data in business and workplace.

The Researcher were asked to put forward some suggestions and the suggestions that the researcher would like to put forward certain suggestions or recommendations:

1. The concept of consent on collecting data must be clearly defined. The way that consent is obtained must be detailed, the parameters needed to make informed consent detailed and the necessity to get explicit, specific consent. Consent must not be put under one umbrella contract or policy. There is a need to get separate consent for separate uses of biometric data. Provisions regarding withdrawal of consent must be made clear. Obtaining consent through writing or contract should be made compulsory and obligatory for every time data is collected.
2. The purpose of collecting like consent must be clearly and specifically provided in details along with the purpose being lawful, legitimate. There
3. In order to maintain transparency and accountability, there is a need to provide for how the data will be processed and information on certain

things to the data subject as categories of data collected, who are the parties that have collected the data- their names, identity, details, etc., ; the parties with access to such data – their identity and details, specific purpose of collection of data, rights of the data subject, on what categories of data are processed and whether it is being processed at the present, how to get a digital copy of their biometric data that is being processes, information about the third parties to whom their data is being transferred or shared, the privacy policy of the organisation before signing of contract or giving written consent through its presence in the contract and website, security and safeguard policies, information on grievance redressal mechanism.

4. There must be clear data retention procedures which defines and details till which period and under what circumstances an organisation can retain biometric data. It must provide clear rules as to when a person stops working in a company or a consumer/ client is no longer using a service, than till what duration after their stopping of such association the company or organisations can retain data and the duration must be used only for settling any remaining purposes or issues.
5. Disposing and erasing of biometric data of a person must be provided upon their wish provided it does not hamper the ongoing purpose and the person has not withdrawn consent or such data is not required by the government. There must be lawful provisions as to whom to approach regarding erasure of biometric data, the parameters needed for such erasure, and the procedures and standards to be maintained when disposing or erasing such data.
6. The data collection limitation must be clearly defined and detailed and there should be a standard in form of a schedule that provides the common standards for collection of any biometric data against any purpose. For e.g., the schedule must contain suppose for what kind of purposes iris recognition can be allowed to be collected, or what kinds of

purposes would require voice recognition, face recognition as well as iris recognition.

7. Accuracy and correctness of biometric data is very important. Periodic review of biometric data annually or once in two years can be provided for correcting and rectifying data.
8. There must be the limitation of government powers. Biometric data details should not be provided to the government just because of law if it violates fundamental rights and there is not enough reason for providing such data. Only for purposes of public interest, scientific research or archival purposes that the data subject has agreed to such biometric data should be provided. It should not be provided for profiling by the government or mass surveillance. Detailed provisions and procedures need to be provided on disclosure of biometric data to government and third parties. Also, the data subject must be informed.
9. The Privacy Policy of the organisations should be given to the data subject or made public through permanent notice and website and for persons who are illiterate or cannot understand, there must be provisions for explaining the privacy policy to them. Companies and organisations have been making their own privacy policies with their own standards. There is a need to make privacy policy compulsory for every organisation and workplace. The law must set comprehensive standards and parameters that the privacy policies must have to include.
10. There is a need to set a separate Biometric Law like BIPA or CCPA for business transactions, commercial transactions and use of biometric authentication in workplace.

As we gear towards a technological future that involves biometrics, AI and all technical innovations that require our personal data, it becomes completely vital to make comprehensive laws regarding both data privacy, biometrics and others. We especially need comprehensive legislature in biometrics regarding to business transactions and workplaces because in the today's global village the people have dealings all over the world and this necessitates data prot

BIBLIOGRAPHY:

I. Books

1. A.K. Jain, P Flynn and A. A. Ross (eds) Handbook Of Biometrics (2nd ed Springer 2007)
2. Samir Nanavati, Michael Thieme and Raj Nanavati, Biometrics Identity Verification in a Networked World, (Wiley Computer Publishing,) 2002
3. Els J. Kindt, Privacy and Data Protection Issues of Biometric Applications ,2013, A Comparative Legal Analysis, Law, Governance and Technology Series, Volume 12, Springer, 2013

II. Cases:

1. Justice K.S. Puttaswamy (Retd.) & Anr v Union of India & Ors ,2019 1 SCC 1
2. Manohar Singh v National Thermal Power Corporation Ltd, 2006 SCC Online CIC 684, Appeal No 80/ICPB/2006
3. Puttaswamy v Union of India , Puttaswamy I, Writ Petition (Civil) No. 494 of 2012,
4. Rosenbach v. Six Flags Entm't Corp., 2019 IL 123186, ¶ 8, 129 N.E.3d 1197, 1200–01

III. Journal Article

1. Amba Kak, Ed., Regulating Biometrics: Global Approaches And Urgent Questions,52-62 (Al Now Institute, 2020),
2. Busch, Christoph. "Facing the future of biometrics. Demand for safety and security in the public and private sectors is driving research in this rapidly growing field." Vol 7 Spec No EMBO reports, S 23-5. (2006) doi:10.1038/sj.embor.7400723
3. Dhira R Duraiswami, 'Privacy and Data Protection in India' (2017) 6 Journal of Law & Cyber Warfare 166, 2017

4. Latha R Nair, 'Data Protection Efforts in India: Blind Leading the Blind' (2008) 4 Indian J L & Tech 19
5. Nayar, Pramod K. "'I Sing the Body Biometric': Surveillance and Biological Citizenship." 2012, vol. 47, no. 32 Economic and Political Weekly, 17–22.
6. Nguyen, Fiona Q. "The Standard for Biometric Data Protection." 2018, Vol 7 no 1. Journal of Law & Cyber Warfare, 61–84.
7. Rahul D Chaudhari, Ashok A Pawar &Rakesh S Deore, The Historical Development Of Biometric Authentication Techniques: A Recent Overview, Vol. 2 Issue 10, IJERT , 3921, 3922-3923 (2013)
8. Singh, Atul. "DATA PROTECTION: INDIA IN THE INFORMATION AGE." (2017) vol. 59, no. 1, Journal of the Indian Law Institute, 78

IV. Statute

1. Aadhar (Enrolment and Update) Regulations , 2016'
2. California Consumer Privacy Act (CCPA)
3. General Data Protection Regulation (GDPR), 2018
4. Illinois Biometric Information Privacy Act
5. The International Covenant on Civil and Political Rights (ICCPR), 1966
6. Information Technology Act
7. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (Privacy Rules)
8. The International Covenant on Civil and Political Rights (ICCPR), United Nations General Assembly Resolution 2200A (XXI), 1966
9. Personal Data Protection Bill, 2019
10. Texas Capture or Use of Biometric Identifier Act (CUBI)

11. United Nations Compendium of Recommended Practices for the Responsible Use and Sharing of Biometrics in Counter-Terrorism, 2018
12. Washington House Bill 1493

V. Online Sources.

1. Biometrics, History of biometrics, HOMELAND SECURITY, https://www.globalsecurity.org/security/systems/biometrics-history.html. (April 30, 2021, 8.00AM),
2. Biometric Consortium, http://www.biometrics.org/, https://web.archive.org/web/20060401033426/http://www.biometrics.org/links.html (July 10, 2021)
3. European Association For Biometrics, About, https://eab.org/ (July 15,2021)
4. History of Biometrics, REFACES.COM, https://recfaces.com/articles/history-of-biometrics (May 1 2021, 8.00AM)
5. John Trader, June 17, 2016, The Top 5 Biometric Associations and Regulatory Bodies Around the World, M2SYS BLOG https://www.m2sys.com/blog/biometric-hardware/top-5-biometric-regulatory-bodies/ (July 17,2021)
6. Mehedi, 25 Uses of Biometric in Today's Society, BIOMETRICTODAY,https://biometrictoday.com/uses-of-biometric-technology-today-society/ (April 12, 2021, 8.00AM)
7. Our History, Biometrics Institute, https://www.biometricsinstitute.org/about/our-history/ (July 17, 2021)
8. Privacy and Biometrics, Biometric Institute, https://www.biometricsinstitute.org/what-is-biometrics/privacy-and-biometrics/ (July 17,2021)

9. Ryan Mac, Caroline Haskins, and Logan McDonald, "Clearview AI Has Promised to Cancel All Relationships with Private Companies," BUZZFEED,) https://www.buzzfeednews.com/article/ryanmac/clearview-ai-no-facial-recognition-private-companies, (July 20, 2021)
10. Suneeth Katarki , Namita Viswanath and Ivana Chatterjee, The Personal Data Protection Bill, 2018 - Key Features And Implications, INDUSLAW, (15 August 2018), https://www.mondaq.com/india/data-protection/727550/the-personal-data-protection-bill-2018--key-features-and-implications (July 22, 2021)
11. Stephen Mayhew, History of Biometrics, BIOMETRIC UPTADE, https://www.biometricupdate.com/201802/history-of-biometrics-2 (April 30, 2021, 8.29P.M)
12. Texas Lawyer, October 5 2020, Meet CUBI—What Companies Need to Know About Texas' Biometric Privacy Law, BLANKROME, https://www.blankrome.com/publications/meet-cubi-what-companies-need-know-about-texas-biometric-privacy-law (July 23,2021)
13. Types of biometrics, BIOMETRICS INSTITUTE, https://www.biometricsinstitute.org/what-is-biometrics/types-of-biometrics/ (July 31, 2021 8.29 PM)

VI. Report

1. Emn Synthesis Report – Immigration Of International Students To The Eu, European Migration Network Study 2012