THE NATIONAL UNIVERSITY OF ADVANCED LEGAL STUDIES, KOCHI

DISSERTATION

Submitted in partial fulfilment of the requirement of the award of degree of

MASTER OF LAW (LL.M)

(2023-24)

ON THE TOPIC

SAFEGUARDING WEARABLE DATA: ASSESSING THE EFFICACY OF DIGITAL PERSONAL DATA PROTECTION ACT 2023

Under the Guidance and Supervision of

Dr. Sheeba. S. Dhar

The National University of Advanced Legal Studies, Kochi

Submitted by:

Ashika Marjan C P

Register No: LM0223006

Roll No: 10526

LL.M (International Trade Law)

CERTIFICATE

This is to certify that Mrs. Ashika Marjan C P, Reg No. LM0223006, has submitted his dissertation titled **"SAFEGUARDING WEARABLE DATA: ASSESSING THE EFFICACY OF DIGITAL PERSONAL DATA PROTECTION ACT 2023"** in partial fulfilment of the requirement for the award of Degree of Master of Laws in International Trade Law to the National University of Advanced Legal Studies, Kochi under my guidance and supervision. It is also affirmed that the dissertation submitted by him is original, bona fide and genuine.

Dr. Sbeeba S Dhar
Supervising Guide
NUALS, Kochi

CERTIFICATE ON PLAGIARISM CHECK

1.	Name of Candidate	Ashika Marjan C P
2.	Title of Dissertation	Safeguarding Wearable Data: Assessing The Efficacy Of Digital Personal Data Protection Act 2023
3.	Name of the Supervisor	Dr. Sheeba S. Dhar
4.	Similar Content Identified	3% (Chapter 1), 9% (Chapter 2 - Parts A-C), 11% (Chapter 2 - Parts D - F), 6% (Chapter 3), 0% (Chapter 4), 5% (Chapter 5), 2% (Chapter 6)
5.	Software Used	Grammarly
6.	Date of Verification	25/06/2024

Checked by: Mr. Sheeba S. Dhar

Name and Signature of the Candidate: Ashika Marjan C P

DECLARATION

I declare that this Dissertation titled "Safeguarding Wearable Data: Assessing The Efficacy Of Digital Personal Data Protection Act 2023" is researched and submitted by me to the National University of Advanced Legal Studies, Kochi in partial fulfilment of the requirement for the award of Degree of Master of Laws in International Trade Law, under the guidance and supervision of Dr. Sheeba S. Dhar, and is an original, bona fide and legitimate work and it has been pursued for an academic interest. This work or any type thereof has not been submitted by me or anyone else for the award of another degree of either this University or any other University.

Ashika Marjan C P
Reg No: LM0223006
LL.M (International Trade Law)
NUALS, Kochi

Date: 25th June, 2024
Place: Kochi

ACKNOWLEDGEMENT

The competition of this dissertation work would not have been possible without the guidance and mentorship of Dr. Sheeba S. Dhar, my guide and supervisor who was a pillar of support throughout. Her regular inputs and meaningful suggestions meant that my work was made much easier than it could have been. I would also like to extend my gratitude to the Vice Chancellor of NUALS, Justice S. Siri Jagan and the Director of Centre for Postgraduate Studies, Prof. Dr. Mini S. Thanks also to all the other faculty members of NUALS, family and friends for their constant encouragement during the course of the writing of this dissertation.

Ashika Marjan C P
LM0223006

LIST OF CASES

- *M.P. Sharma & Ors. vs. Satish Chandra and Ors(1954) 1 SCR 1077*
- *Kharak Singh vs State of Uttar Pradesh AIR 1963 SC 1295.*
- *R. Rajagopal & Ors. vs. State of Tamil Nadu & Ors., AIR 1995 SC 264.*
- *Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors., AIR 2017 SC 4161*
- Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems C-311/18, ECLI:EU:C:2020:559

.

TABLE OF CONTENTS

CHAPTER I

INTRODUCTION

Wearable technology is any kind of electronic device designed to be worn on the user's body. Such devices can take many forms, including jewellery, accessories, medical devices, and clothing or clothing elements. They are usually worn close to the skin — to accurately relay necessary medical, biological and exercise data to a database. Fitbit and Google Glass are some examples of wearable technology. The most sophisticated examples of wearable technology include artificial intelligence hearing aids, Google Glass, Microsoft's HoloLens, and a holographic computer in the form of a virtual reality (VR) headset.

A new report from Cientifica Research, Smart Textiles and Wearables: Markets, Applications and Technologies, examines the markets for textile-based wearable technologies, the companies producing them and the enabling technologies[1]. The report identifies three distinct generations of wearable technologies:
1.First generation is where a sensor is attached to wearable and is the approach currently taken by significant sportswear brands such as Adidas, Nike and Under Armour 2. Second-generation products embed the sensor in the wearable, as demonstrated by Samsung, Alphabet, Ralph Lauren and Flex products. 3. In third-generation wearables, the garment itself is the sensor, and a growing number of companies, including AdvanPro, Tamicare and BeBop sensors, are making rapid progress in creating pressure, strain and temperature sensors.

The rapid proliferation of wearable technology, from smartwatches to fitness trackers, has ushered in a new era of pervasive data collection, which is also known as wearable data, raising significant concerns regarding the security and privacy of personal information. Within this context, the "Digital Personal Data Protection Act 2023" in India emerges as a robust framework seeking to safeguard the privacy rights of its citizens. The Digital Personal Data Protection Act of 2023 represents a seminal piece of legislation aimed at safeguarding the privacy and security of individuals' personal data within the digital realm. This Act establishes

[1] Cientifica Ltd (Publisher), April 2019, 'Smart Textiles and Nanotechnologies: Appplications, Technologies and Markets', www.cientifica.com

a comprehensive legal framework that addresses the challenges and necessities of data protection in the age of digital transformation. It emphasises individuals' rights to their data, delineating clear obligations and responsibilities for data handlers and processors to ensure transparency, security, and accountability in data practices. This dissertation delves into the efficacy of the said Act in protecting the data collected and generated by wearable technologies (wearable data). A comprehensive analysis explores how the legislation addresses the intricate challenges posed by these devices, evaluates its strengths and weaknesses, and investigates its real-world implications for users, manufacturers, and policymakers. The study aims to provide a nuanced understanding of the intersection between cutting-edge technology and privacy laws, offering valuable insights into the evolving landscape of digital data protection in India. This research focuses on wearable technology's legal implications, specifically data privacy and protection under the Digital Personal Data Protection Act 2023.

1.1 SCOPE OF THE STUDY

The study aims to analyse how the Digital Personal Data Protection Act (DPDPA) 2023 in India address the evolving challenges posed by wearable technology in terms of data privacy and protection, as well as to examine the legislative gaps. It also compares data protection regulations from other jurisdictions that effectively address wearable technology. It seeks to provide actionable insights for policymakers, industry stakeholders, and researchers interested in enhancing privacy safeguards within the wearable technology landscape.

1.2 OBJECTIVES

- To analyse data protection and privacy issues in wearable technology and to examine the legal concerns they pose within the wearable technology industry's privacy landscape.
- To conduct an analysis of data privacy regulations and standards related to wearable technology in India under the Digital Personal Data Protection Act 2023.
- To analyse and Compare data protection regulations from other jurisdictions that effectively address wearable technology.

1.3 RESEARCH QUESTIONS

- What are the recent security and privacy issues in wearable technology, and how do these issues raise legal concerns related to privacy matters in the field of wearable technology?
- How efficient are the data privacy regulations and standards in India under the Digital Personal Data Protection Act 2023?
- How do data protection regulations in various jurisdictions compare in their approach to regulating wearable technology?

1.4 HYPOTHESIS

Regulations under the Digital Personal Data Protection Act 2023 exhibit gaps in safeguarding digital data privacy in wearable technology devices.

1.5 RESEARCH METHODOLOGY

The research is purely doctrinal but will make use of already available statistical data wherever necessary. The research relies on legal documents, technological documents, and the available literature. This research will depend upon secondary data released by international institutions, journals, books and other peer-reviewed articles.

1.6 CHAPTERISATION

Chapter 1: Introduction

Introduce the concept of wearable technology and its growing significance. Highlight the importance of data privacy in the context of wearable technology.

Chapter 2: Wearable Technology and its Data Landscape

Delve into various types of wearable technology, focusing on the unique data each type collects. (e.g., fitness trackers collect health data, smartwatches collect location data).Discuss

the sensitivity of data collected by wearables, emphasizing the potential privacy risks associated with its collection, processing, storage, and sharing.

Chapter 3: Digital Personal Data Protection Act 2023

Analyse the strengths of the DPDPA 2023 in protecting personal data in general. Discuss key provisions of the act, such as consent, data minimization, and data breach notification, highlighting their effectiveness in broader data protection.

Chapter 4: The DPDPA 2023 and the Gaps in Wearable Data Protection

Identify specific areas where the DPDPA falls short in addressing the unique data collection practices of wearable technology. Discuss the act's shortcomings in addressing data security concerns specific to wearables, proposing amendments (e.g., stricter encryption standards).

Chapter 5: Global Best Practices

Compare and contrast data protection regulations from other jurisdictions that effectively address wearable technology.

Chapter 6: Conclusion

Summarize the key findings of the research, emphasizing the identified flaws in the DPDPA's application to wearable data. Discuss the potential consequences of inadequate data protection for wearables. Propose concrete recommendations for strengthening the DPDPA or introducing new regulations specific to wearable technology, incorporating best practices identified in Chapter 5.Conclude by emphasizing the importance of robust data protection frameworks for a thriving wearable technology ecosystem that fosters trust and innovation.

1.6 LITERATURE REVIEW

- Marie Lamensch, August 2021, Montreal Institute for Genocide and Human Rights Studies at Concordia University Journal “Putting Our Bodies Online: The Privacy Risks of Teach Wearables
- “As researchers at the Edmond J. Safra Center for Ethics have found, there are long-term implications to the “surveillance of the human body by governments, private companies, governments, employers and other entities who have a stake in our data.”

- Michael McCarthy,2023 BMJ Publishing Group Ltd, Federal privacy rules offer scant protection for users of health apps and wearable devices
- “The report, which was mandated by Congress, was prepared by the US Department of Health and Human Services, Office of the National Coordinator for Health Information Technology, with support from several other agencies said that, “While technological innovation has advanced at an extraordinary pace in recent years, privacy and security protections of health information have not kept up

- Kagalwalla, N., Garg, T., Churi, P., & Pawar, A. (2019). A survey on implementing privacy in healthcare: An Indian perspective.International Journal of Advanced Trends in Computer Science and Engineering
- “With the advent of the technology of wearable devices which captures the real-time health data, we cannot ignore the privacy concerns.”

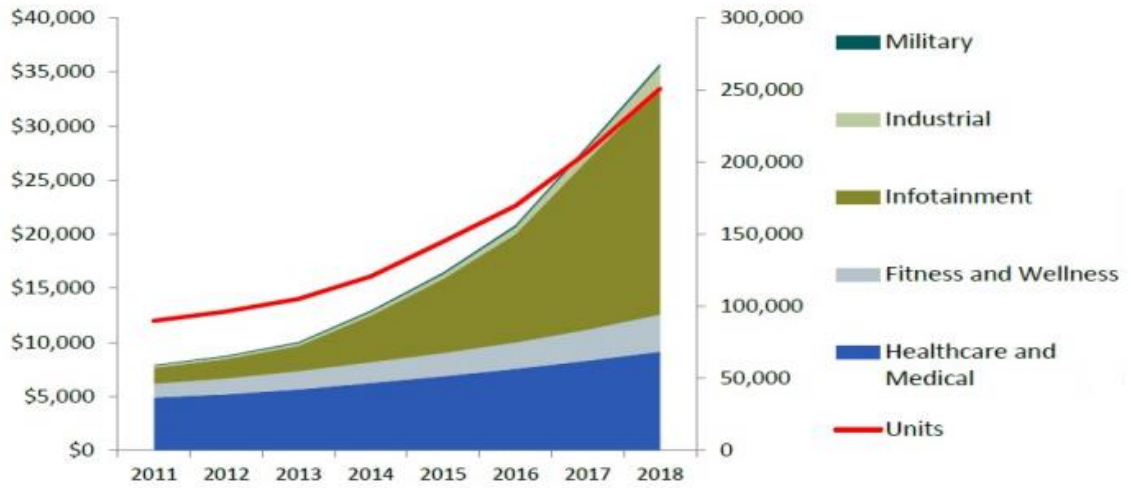
CHAPTER 2

WEARABLE TECHNOLOGY AND ITS DATA LANDSCAPE

2.1 INTRODUCTION

Wearable devices have received lot of attention lately, and many vendors - including big names such as Google - are throwing their hats into the wearable market. A wearable device is an electronic device capable of storing and processing data that is incorporated into a person's clothing or personal accessories. The most promising applications in wearable devices market are infotainment, fitness and healthcare. Because these applications can satisfy people's needs of life and are easily controlled with smart devices like smart phones. According to IHS, there will be 250 million wearable devices in 2018, most of them are applied in the three vertical markets. The service revenue will exceed $6 billion in 2018 inclusive of remote patient monitoring, support for gaming and enterprise applications, and military research.[2]

Fig.9 World market for wearable devices and service($millions,000 units)



Source: IHS

[2] Shan, Li, and Chen Pei. "Internet of Things (IOT) Development for the Promotion of Information Economy," November 2015.

Wearable devices, from fitness trackers to smartwatches, are constantly gathering information about . This data offers a wealth of insights, but understanding its vastness can be overwhelming.This chapter will delve into the diverse data landscape of wearable technology. We will uncover the various types of data collected by these devices, ranging from biometric information like heart rate and blood pressure to environmental data like temperature and air quality. We'll also explore how wearables track our activity levels, sleep patterns, and even our movements through GPS and biomechanical sensors. As this technology continues to evolve, the possibilities for data collection, and the potential benefits it offers, are constantly expanding.

2.2 DATA COLLECTION AND STORAGE

Wearable devices collect a vast amount of personal health data, including physiological parameters, location information, and behavioral patterns. This data is often stored in the cloud, and third-party access is granted to companies and researchers who may use this data for various purposes, such as marketing, research, or healthcare management. The sheer volume and sensitivity of this data raise concerns about data privacy and security, as unauthorized access or misuse can have severe consequences for individuals and society as a whole.

2.3 TYPES OF DATA COLLECTED

- **Biometric Data:** This includes information about the wearer's body such as heart rate, blood pressure, respiratory rate, and body temperature. Wearables often feature sensors like optical heart rate monitors, accelerometers, and gyroscopes to track these metrics.There are many forms of biometrics that are in wide-scale use for both identification and authentication of individuals. For example, fingerprint technology is used in applications from access control of electronic devices to the tracking of individuals involved in criminal activity. An individual's iris pattern is another biometric frequently used for authentication purposes, including passport control.

  Both fingerprint and iris are an example of static biometric data, whereby the observed characteristic is static and is mostly stable, except for slow deterioration due to ageing or injury. There are, however, dynamic biometric measures which are linked to individuals behavioural and biological characteristics. For example, an individual's written signature and their voice can be used as biometric measures. However, it is often the case that

dynamic biometrics can suffer from reduced accuracy because of variation in samples and poor repeatably (i.e., an individual's signature is likely to have small differences every time).[3]

Each biometric source involves a different collection method. For example, an iris pattern requires a photo to be taken, whereas a fingerprint requires a map of high/low markings. Taking a photo of an iris pattern is regarded as passive as it does not require too much involvement from the individual, whereas providing a fingerprint through a mechanism whereby an individual has to place their fingerprint on a reader is classed as invasive. In general passive biometrics are regarded as the most user-friendly; however, they often suffer from a reduced accuracy. Biometric systems aiming to use health data based on behavioural and biological characteristics are using data that is not classified as static. It is also the case that for the majority of applications, physical contact is required to sense the necessary information. The use of behavioural and biological characteristics, coupled with multiple sensing mechanisms of different accuracy, results in it being challenging to implement a biometric system.[4]

- **Activity and Movement Data:** Wearables track physical activity and movement patterns, including steps taken, distance traveled, calories burned, and active minutes. Accelerometers and gyroscopes are commonly used to monitor motion and activity levels. A wearable tracker continuously senses the movements of the body on a 3 axis accelerometer. The data is recorded all the time it is worn and powered up, which enables the tracker to trace if the individual is walking forward, running fast, or even standing stil All this data is stored in the tracker for further processing. Processing occurs when the data is transferred to the software associated with the fitness tracker on the smartphone or laptop with which it is synced.[5]Since the individual has already shared personal details with the software, the data collected is run through a personalized algorithm. This makes it possible for the software to detect what the different movements recorded actually imply.

[3] Khan, Saad, Simon Parkinson, Liam Grant, Na Liu, and Stephen Mcguire. "Biometric Systems Utilising Health Data from Wearable Devices." ACM Computing Surveys 53, no. 4 (July 11, 2020): 1–29. https://doi.org/10.1145/3400030.
[4] ibid
[5] News-Medical. "How do wearable fitness trackers measure steps?," April 7, 2023. https://www.news-medical.net/health/How-do-wearable-fitness-trackers-measure-steps.aspx.

- **Sleep Data**: Many wearable devices are designed to monitor sleep patterns, including duration, quality, and stages of sleep such as deep sleep, REM (rapid eye movement) sleep, and light sleep. These devices often use accelerometers and heart rate monitors to detect movement and changes in heart rate during sleep

  Actigraphy devices (mainly wrist-worn devices) rely on an accelerometer to measure patterns of activity (motion) and estimate sleep/wake states accepting the simple assumption that motion implies wake, and no-motion implies sleep. Due to their small size, comfort and waterproof properties, actigraphy devices are designed to be worn 24/7 and thus are suitable for prolonged recordings in non-laboratory settings. The device's accelerometer detects the occurrence and degree of motion in multiple directions (e.g., 3-axis), which is converted into a digital signal to derive an activity count. Then, depending on the sleep-wake threshold of the algorithm, an epoch is determined as wake if its activity count exceeds the threshold, or sleep if it is below the threshold. Data can be stored at different rates, which contributes to how long a device can store continuous data.[6]

- **Environmental Data:** Some wearables are equipped with sensors to collect environmental data such as temperature, humidity, UV exposure, and air quality. This data can provide insights into the wearer's surroundings and potential health risks.In total, 22 different environmental parameters are measured by G1 devices. Temperature and humidity are measured by 23 and 22 devices, respectively. Nine devices measure CO, NO, and VoCs, which indicates the importance of air pollutants in environmental monitoring. Particular matter, pressure, and U are, each integrated in / devices. CO and SO are integrated into 6 and 4 devices, respectively. UV and light are measured by 3 devices[7]

  In a study of G1 wearables, it was found that 34% of the devices are waist-worn, making it the most popular option, followed by 23% worn on the wrist or arm. Other forms, like garments, account for 20% of the devices. Bluetooth is the dominant communication protocol, used by 31% of devices. Data from these devices is most commonly sent to smartphones or the cloud/server (32%), with some transmitting to PCs (23%) and a few

[6] De Zambotti, Massimiliano, Nicola Cellini, Aimée Goldstone, Ian M. Colrain, and Fiona C. Baker. "Wearable Sleep Technology in Clinical and Research Settings." Medicine and Science in Sports and Exercise 51, no. 7 (February 19, 2019): 1538–57. https://doi.org/10.1249/mss.0000000000001947.

[7] Haghi, Mostafa, Saeed Danyali, Sina Ayasseh, Ju Wang, Rahmat Aazami, and Thomas M Deserno. "Wearable Devices in Health Monitoring from the Environmental towards Multiple Domains: A Survey." Sensors 21, no. 6 (March 18, 2021): 2130. https://doi.org/10.3390/s21062130.

storing data locally (14%). The primary use of these wearables is general monitoring (69%), with specific diagnostics and disease management each making up 11%, and a small portion (9%) for non-medical applications.[8]

- **GPS and Location Data:** Wearables with GPS capabilities can track the wearer's location and movement in real-time. This data is commonly used for fitness tracking, navigation, and location-based services. Wearable technology typically collects location and GPS data through built-in GPS sensors or by syncing with the GPS capabilities of paired smartphones. These sensors track the wearer's movements and provide accurate location data, which can then be used by various applications and services on the device. Additionally, some wearables may also use Wi-Fi or cellular triangulation to enhance location accuracy in areas with poor GPS reception.

  By integrating a range of sensors, including accelerometers, gyroscopes, Bluetooth, WiFi, and GPS, a comprehensive tracking system can efficiently monitor users' activities both indoors and outdoors, which can help depict a comprehensive storyline of patients' daily routines and behaviors. In our application, the accelerometer is utilized to continuously capture data in the background, determining whether the wearer is in motion or stationary using a pretrained classifier embedded on the watch. When the user is stationary, the data collection application conserves battery power by excluding the reading of location-related sensors, focusing solely on the accelerometer to identify potential changes in physical activity

- **Biomechanical Data:** Advanced wearable devices, especially those used in sports and athletics, may collect biomechanical data related to posture, gait analysis, and movement efficiency. This information can be valuable for optimizing performance and preventing injuries.

  These sensors can be mounted to different parts of human body, for example, the chest, waist, and upper and lower limbs, and can even be worn in pockets or shoes or adhered to the skin to collect data quickly and conveniently for the human motion of interest. In addition, sensors are integrated into wearable devices, such as orthoses and exoskeletons, applicable for patients with hemiplegia, elderly people, and workers, with the purpose of

[8] Ibid

assistive control. Many wearable sensors have been developed over the years and can be classified by signal source into three major categories: electromechanical sensors, bioelectrical sensors, and biomechanical sensors. Sensors that detect limb motion and collect kinematic and kinetic information include accelerometers, encoders (angle, angular velocity, linear acceleration, angular acceleration, inclination angle), inertial measurement units (IMUs) with even more kinematic data, and foot switches and pressure insoles.

- **Emotional and Stress Data:** Emerging wearable technologies are exploring the collection of emotional and stress-related data through sensors that detect changes in skin conductivity, heart rate variability, and other physiological signals associated with emotional states. The nervous system responds to stress, which directly affects eye movements and sweat secretion. Therefore, the changes in brain potential, eye potential, and cortisol content in sweat could be used to interpret emotional changes, fatigue levels, and physiological and psychological stress. To better assess users, stress-sensing devices can be integrated with applications to improve cognitive function, attention, sports performance, learning ability, and stress release. These application-related wearables can be used in medical diagnosis and treatment, such as for attention-deficit hyperactivity disorder (ADHD), traumatic stress syndrome, and insomnia, thus facilitating precision medicine. Gel is usually essential for detecting brain waves, as gel diminishes the impedance between the skin and the electrode surface. However, the gel hinders the use of brainwave detectors as wearable devices because gel leaves residues on the scalp, and electrode leakage could result in a short circuit between adjacent electrodes. Furthermore, gel dries out during prolonged use, resulting in a decrease in the EEG signal value[9]. Therefore, semidry or dry electrodes must be developed to replace gel-type wet electrodes[10]. Dry electrodes can be divided into three categories: contact electrodes, noncontact electrodes, and insulated electrodes. The main difference between noncontact and insulated electrodes is that the bottom of the insulated electrode is composed of insulating material. In contrast, noncontact electrodes are formed of metal and can be

[9] Ferree, Thomas C, Phan Luu, Gerald S Russell, and Don M Tucker. “Scalp electrode impedance, infection risk, and EEG data quality.” Clinical Neurophysiology 112, no. 3 (March 1, 2001): 536–44. https://doi.org/10.1016/s1388-2457(00)00533-2.

[10] Li, Guang-Li, Jing-Tao Wu, Yong-Hui Xia, Quan-Guo He, and Hong-Guang Jin. “Review of semi-dry electrodes for EEG recording.” Journal of Neural Engineering 17, no. 5 (October 1, 2020): 051004. https://doi.org/10.1088/1741-2552/abbd50.

coupled with hair or clothing. Although the signal quality of contact electrodes is better, noncontact and insulated electrodes are easier to apply in wearable devices.[11]

- **Audio and Voice Data:** Smart wearable devices with microphones can capture audio and voice data for features like voice commands, dictation, and voice-controlled interactions with virtual assistants.It is the heart of a Voice application system, which has ability to understand voice input given by user, and make application work in a efficient way and generating voice feedback to the user. This system is an important component for user as a gateway to use his or her voice as a input component. In a Nutshell, for clearly understanding user voice command and to get feedback from the system, we should consider voice recognition system contains all the process by which application system directs for building speech signals to text data and few form of important meaning of speech. Voice-Controlled Devices uses Natural Language Processing to process the language spoken by the human and understand the query and process the query and respond to the human with the result. The understanding of the device means Artificial Intelligence needs to be integrated with the device so that the device can work in a smart way and can also control IoT applications and devices and can also respond to query which will search the web for results and process it. It is designed to minimize the human efforts and control the device with just human Voice. The device can also be designed to interact with other intelligent voice-controlled devices like IoT applications and devices, weather reports of a city from the Internet, send an email to a client, add events on the calendar, etc. The accuracy of the devices can be increased using machine learning and categorizing the queries in particular result sets and using them in further queries. The accuracy of the devices is increasing exponentially in the last decade. The devices can also be designed to accept commands in bilingual language and respond back in the same language queried by the user. The device can also be designed to help visually.

  It's important to note that the collection and processing of personal data by wearable technologies raise privacy and security concerns. Users should be aware of how their data

[11] Wu, Ju-Yu, Congo Tak-Shing Ching, Hui-Min David Wang, and Lun-De Liao. “Emerging Wearable Biosensor Technologies for Stress Monitoring and Their Real-World Applications.” Biosensors 12, no. 12 (November 30, 2022): 1097. https://doi.org/10.3390/bios12121097.

is being collected, stored, and used, and companies must adhere to relevant privacy regulations to protect user privacy and data security.

2.4 LEGAL ISSUES

However, these advancements also raises certain legal concerns the collection, storage, and use of personal data.

- Privacy Concerns: Wearable devices are designed to collect and store sensitive data on the devices themselves and also usually on the connected smartphone. This raises concerns about data privacy and security. Users do not have any control over what their device's manufacturer might do with their data, and third parties could intercept the data during transmission or gain access to the data stored in the device and the connected smartphone[12].Additionally, the data collected by wearable devices may be vulnerable to interception during transmission or unauthorized access while stored on the device or connected smartphone. This can lead to serious consequences, such as identity theft, financial fraud, or reputational damage Users expressed the need for having shorter terms and conditions that are easier to read, a more understandable informed consent form that involves regulatory authorities and there should be legal consequences on the violation or misuse of health information provided to Wearable Devices. Google Glass an augmented reality device is currently facing privacy issues relating to use of data by third parties. Bars and casinos have already banned the use of this technology on their premises due to patrons being photographed and having their images recorded without their consent. Security and privacy risks can deal with a patient's health by causing intentional malfunction of the device. Data integrity can be compromised because sensor-based technology is still in adevelopment stage andcorrupt data can be produced.[13]
- Data Ownership and Control: Users need clarity on who owns the data generated by wearables. Is it the user, the device manufacturer, or the service provider? Legal frameworks must address data ownership and control rights to ensure that users have

[12] Ernst, Claus-Peter Hermann and Alexander W. Ernst. "The Influence of Privacy Risk on Smartwatch Usage." Americas Conference on Information Systems (2016).
[13] Kapoor, Vidhi & Singh, Rishabh & Reddy, Rishabh & Churi, Prathamesh. (2020). Privacy Issues in Wearable Technology: An Intrinsic Review. SSRN Electronic Journal. 10.2139/ssrn.3566918.c

control over their personal data and can make informed decisions about its use and sharing

- Informed Consent: Wearable users must be informed about data collection practices and provide explicit consent before their data is collected and shared. Transparency is vital to ensure users understand how their data is used and shared, and to prevent unintended consequences. Informed consent is a fundamental ethical principle that must be respected to maintain trust in wearable technology.[14]
- Data Security: Protecting wearable data from breaches or unauthorized access is critical. Legal requirements for data encryption, storage, and transmission must be established to ensure the confidentiality, integrity, and availability of personal data. Data security measures, such as secure data storage and two-factor authentication, must be implemented to prevent data breaches and unauthorized access.
- Health Regulations: Wearables used for health monitoring may fall under medical device regulations. Compliance with safety standards and accuracy requirements is critical to ensure the reliability and effectiveness of health-related data. [15]Health regulations must be adapted to address the unique challenges posed by wearable technology, including data quality and accuracy, interoperability, and health equity.
- Liability: If wearable data influences decisions, such as health diagnosis, legal questions arise about liability. Who is liable if incorrect data leads to adverse outcomes? Legal frameworks must address liability issues to ensure accountability and protect users' rights. Liability must be clearly defined to prevent disputes and ensure that users can trust wearable technology to provide accurate and reliable health information..

2.5 ETHICAL CONCERNS

The ethical concerns surrounding wearable digital health technology are multifaceted and far-reaching. Firstly, the collection and storage of personal health data without informed consent can be seen as a violation of individuals' privacy and autonomy. Secondly, the lack of transparency and accountability in data handling and processing can lead to mistrust and

[14] Panayiotou, Andrie G., and Evangelos D. Protopapadakis. “Ethical issues concerning the use of commercially available wearables in children: Informed consent, living in the spotlight, and the right to an open future.” *JAHR* 13/1, no. No. 25 (2022).

[15] Bouderhem, Rabaï. 2023. "Privacy and Regulatory Issues in Wearable Health Technology" *Engineering Proceedings* 58, no. 1: 87. https://doi.org/10.3390/ecsa-10-16206

skepticism among users. Thirdly, the potential for data breaches and cyber attacks can result in serious consequences, such as financial loss or damage to an individual's reputation.[16]

One of the primary ethical concerns with wearable digital health technology is data collection and storage. As these devices track and monitor personal health data, they collect a significant amount of personal data. This data is often stored in the cloud, and third-party access is granted to companies and researchers who may use this data for various purposes. This can lead to concerns regarding data privacy and security.[17]

2.6 CONCLUSION

The extensive data collection of wearable devices includes not only physiological measurements but also movement patterns, raising significant privacy and security concerns due to its sensitivity and volume. Diverse biometrics, ranging from static, like fingerprints, to dynamic, such as voice or signature, underscore the challenges in maintaining accuracy and privacy in biometric systems. Wearable devices that monitor sleep patterns utilize accelerometers and heart rate monitors to track movement and physiological changes during different sleep stages, offering a comprehensive view of sleep quality and duration. Environmental sensors included in some wearables measure a variety of parameters, including temperature and air quality, to provide insights into the wearer's surroundings and potential health impacts. The application of GPS and additional sensors in wearables allows for accurate tracking of location and physical activity, facilitating fitness monitoring and navigation, and can adjust data collection based on the wearer's activity levels to conserve battery life. Moreover, the collection of biomechanical data by wearables, through sensors placed on various body parts, can aid in sports and athletics by optimizing performance and preventing injuries through posture and movement analysis. Wearable technologies are increasingly capable of collecting complex emotional, stress-related, and auditory data, offering potential benefits in healthcare, personal well-being, and interactive technology applications. However,

[16] Rosie Dobson et al., "Use of Consumer Wearables in Health Research: Issues and Considerations," JMIR. Journal of Medical Internet Research/Journal of Medical Internet Research 25 (November 21, 2023): e52444, https://doi.org/10.2196/52444.

[17] "Privacy Data Ethics of Wearable Digital Health Technology," Center for Digital Health | Engineering | Brown University, May 4, 2023, https://cdh.brown.edu/news/2023-05-04/ethics-wearables.

these advancements also necessitate stringent privacy and security measures to address significant concerns regarding the collection, storage, and use of personal data.

The legal and ethical concerns related to the advancement of wearable digital health technology, includes issues such as privacy, data ownership, informed consent, data security, health regulations, and liability. It is important to protect users' sensitive data from unauthorized access or breaches and ensuring that users have control over their personal data with clear legal frameworks. Ethical issues include the violation of privacy and autonomy from collecting and storing health data without informed consent, the potential for data breaches, and the lack of transparency in data handling. There is a need for understandable terms and conditions, regulatory involvement in consent processes, and legal consequences for the misuse of health information to maintain trust in wearable technology.

CHAPTER 3

DIGITAL PERSONAL DATA PROTECTION ACT 2023

3.1 INTRODUCTION

In the rapidly evolving digital world, the advent of wearable technology has brought forth a new frontier in the collection and analysis of personal data. With devices that can monitor everything from our heart rates to our sleep patterns, the question of how to protect this sensitive information is more pertinent than ever. This is where the Digital Personal Data Protection Act 2023 (DPDPA 2023) steps in, providing a comprehensive legal framework aimed at safeguarding the privacy rights of individuals. Chapter 3 delves into the strengths of the DPDPA 2023, examining how the legislation not only addresses the unique challenges posed by wearable technologies but also sets a precedent for data protection in the digital age.

3.2 CONCEPT OF PRIVACY

Bridging the gap between the critical importance of privacy and the rapid advancements in technology, the question of how wearable technology intersects with the right to personal privacy emerges as a pressing concern in our digitally-driven society.But, how do we ensure this right is being protected at any cost? Coming up with a cure for a disease is not always an easy task, especially when a term like 'privacy' is dynamic and its interpretation also varies with the progression of society.

The notion of privacy in India has its roots in the country's constitutional framework and the evolution of its jurisprudence. Initially, the Supreme Court's rulings in cases like *Kharak Singh v. State of Uttar Pradesh* (1964)[18] and *M.P. Sharma v. Satish Chandra* (1954)[19] had held that there was no explicit fundamental right to privacy under the Indian Constitution . However, this position underwent a gradual shift as the courts began to recognize privacy as an essential component of other fundamental rights.In the landmark case of *R. Rajagopal v. State of Tamil Nadu* (1994)[20], the Supreme Court acknowledged the right to privacy as a part of the right to

[18] Kharak Singh vs State of Uttar Pradesh AIR 1963 SC 1295
[19] M.P. Sharma & Ors. vs. Satish Chandra and Ors (1954) 1 SCR 1077
[20] R. Rajagopal & Ors. vs. State of Tamil Nadu & Ors., AIR 1995 SC 264.

life and personal liberty under Article 21 of the Constitution . The court held that the right to privacy is not an absolute right and can be restricted by the state for legitimate purposes.

The turning point in the recognition of privacy as a fundamental right came in 2017, with the Supreme Court's landmark judgment in *Justice K.S. Puttaswamy (Retd.) v. Union of India*[21] . In this case, a nine-judge bench unanimously held that the right to privacy is a fundamental right protected under Articles 14, 19, and 21 of the Constitution.The court's ruling overturned its previous decisions in *Kharak Singh* and *M.P. Sharma*, stating that the right to privacy is an intrinsic part of the right to life and personal liberty. The judgment emphasized that privacy is essential for the meaningful exercise of other fundamental freedoms and is a necessary condition for the protection of human dignity and liberty.The *Puttaswamy* judgment has had far-reaching implications for the protection of privacy in India. It has paved the way for the development of a comprehensive data protection framework, as the court called for the government to create a robust data protection regime to safeguard individual privacy.However, the implementation of this framework has faced several challenges. The government's introduction of the Personal Data Protection Act, which aimes to regulate the processing of personal data.

Keeping up with its never-giving-up spirit, India has finally gotten its new privacy law, The Digital Personal Data Protection Act 2023 (DPDPA), issued by the Ministry of Electronics and Information Technology (MeitY).[22]The DPDPA aims to create a regulatory framework for the processing, storage, and transfer of digital Personal data, either collected online or offline which was then digitalized.[23] It has prescribed rules and set accountability for various companies or Data Fiduciaries to comply while elaborating on the rights and duties of the data holders or Data Principals, non-fulfillment of which attracts heavy penalties.[24] Digital Data refers to any form of information or content that is stored in, or processed, in a computer system or computer network.[25] Dedicated legislation on personal data in itself is enough evidence to

[21] Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors., AIR 2017 SC 4161.
[22] Khilansha Mukhija and Shreyas Jaiswal, “Digital Personal Data Protection Act 2023 in light of the European Union’s GDPR,” Jus Corpus Law Journal, November 7, 2023, 312–14.
[23] Ashneet Hanspal, “Analysis Of The Digital Personal Data Protection Bill, 2022,” January 4, 2023, https://www.mondaq.com/india/data-protection/1267190/analysis-of-the-digital-personal-data-protection-bill-2022.
[24] “The Digital Personal Data Protection Bill, 2023,” PRS Legislative Research, n.d., https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023.
[25] Adv Swati Sinha, 'Data Protection Law in India- Needs and Position' (Legal Services India, 25 November 2022) accessed 18 September 2023

establish the kind of power it holds today; given we have deeply delved into the digital realm. Digital interactions have become frequent and integral, to the extent that it is capable of holding and controlling the identity of an individual to the world at large. According to Westin, the ever-increasing practice of computerizing personal records needs laws to be adapted to safeguard the rights and prevention of breaches of those rights, well in time.[26] The new legislation mentions that digital personal data should be used only for the purpose for which it is collected and that too, should be lawful, fair, and transparent, and hence, it restricts its unauthorized use, giving a sense of rightful ownership to the data principals. The landmark judgment Justice K.S Puttaswamy (Retd.) and Anr v Union of India (2017) popularly known as the Aadhaar case, formed the precedent of this particular intention of the legislation, wherein the Supreme Court, although validating the much contested Aadhaar Act, clearly recognized the right to privacy as a fundamental right protected under Article 21 of the Indian Constitution, where the emphasis was given on the importance of protection of personal data from unauthorized use. The judgment also reflected the need for data protection laws to safeguard individuals' privacy.

Later on, in 2018, the Supreme Court expanded its earlier judgment and declared the Aadhaar project, a biometric-based national identification system, should not infringe on the right to privacy, emphasizing the importance of obtaining informed consent for data collection and processing.[27] Hence, it is safe to say that the new legislation has inculcated some salient features that shall be systematically examined further in this research.

The processing of personal data helps comprehend individual preferences, which can be beneficial for personalized customization, targeted advertising, and providing recommendations. It can also aid in law enforcement efforts. However, if not regulated, the processing of personal data can have negative consequences on individual privacy, acknowledged as a fundamental right . Unchecked processing could expose individuals to potential harm, including financial losses, damage to their reputation, and profiling. And that's why it became critical for the country to come up with an act that can regulate data protection. Currently Information Technology (IT) Act, 2000, is the act regulating personal data and data

[26] Luisa Rollenhagen, "Alan Westin is the father of modern data privacy law," Osano, January 15, 2021, https://www.osano.com/articles/alan-westin.
[27] Rachit Garg, "Constitutional validity of Aadhar Act in the case of Justice K.S. Puttaswamy (Retd.) and Anr. Vs. Union of India - iPleaders," iPleaders, September 14, 2022, https://blog.ipleaders.in/justice-k-s-puttaswamy-retd-and-anr-vs-union-of-india/.

protection. However in 2017, the government established a panel of experts chaired by Justice B. N. Srikrishna to investigate issues concerning data protection in the country. The panel presented its report8 in July 2018. Taking into account the panel's recommendations, the Personal Data Protection Bill9 of 2019 was introduced in the Lok Sabha in December 2019. The bill was then referred to a Joint Parliamentary Committee, which delivered its report in December 2021. However, in August 2022, the bill was withdrawn from Parliament. Subsequently, in November 2022, a Draft Bill was made available for public feedback. Finally, in August 2023, the Digital Personal Data Protection Bill of 2023 was introduced in Parliament and subsequently got implemented. This paper presents a comprehensive examination of the recently implemented Digital Personal Data Protection Act 2023. The Act stands as a concise and streamlined legal framework that reflects India's standpoint concerning data protection principles in relation to the obligations and functions of both individuals and businesses. It sheds light on the fundamental aspects of the Act that organizations must consider prior to embarking on their endeavors towards achieving privacy compliance.

3.3 SALIENT FEATURES OF THE ACT

- **Language and structure of the Act:**

The language and structure of the Act have been kept simple, to aid a clear understanding of all the provisions, keeping in mind the technical nature of the subject matter and its scope. It sets our various definitions like Data fiduciary, Data principal, data processor, gain, loss, harm, etc. These definitions help in a comprehensive understanding of the scope and nature of its provisions in the Act. The Act negates any unauthorized collection of personal data by the data fiduciaries and allows the processing, storage, or transfer of data, as per relevant provisions, only for the purpose for which it is collected.

- **Scope of the Act:**

According to Section 3 (a), the scope of the Act extends to the handling of personal data in digital form within India. This includes instances where (i) the data is gathered through online means or is (ii) collected offline and subsequently converted into digital format. The Act’s jurisdiction also encompasses data processing outside India if it pertains to providing goods or services to data principals10 within the country.

However, this section grants exceptions for the handling of personal information in instances when:

- An individual utilizes the data for personal or household reasons.
- Personal information has been disclosed by the data subject or due to a legal mandate.
- Personal data required for research, archiving, or statistical objectives, provided it is not employed for specific decisions related to the data subject and the processing conforms to government-defined benchmarks.

- **Personal Data**

Personal data[28] is defined as any data about an individual who is identifiable by or in relation to such data. Digital Personal data means personal data in digital form. Processing[29] in relation to personal data, means a wholly or partly automated operation or set of operations performed on digital personal data, and includes operations such as collection, recording, organisation, structuring, storage, adaptation, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction. Thus Personal data refers to information that pertains to an identified or identifiable person. Both businesses and government organizations handle personal data to provide goods and services.

- **Obligations[30] of Data Fiduciaries**

The Act has recognized an additional category as Significant Data Fiduciary based on several factors such as sensitivity, volume, potential impact, etc. for which the central government has been empowered for classification. The provision has provided additional obligations for significant data fiduciaries as it recognized the importance of safeguarding certain kinds of data. Measures such as periodic Audits by an Independent Data Auditor and Data Protection Impact Assessments have been undertaken.

[28] section 2 (t) of the DPDP Act, 2023.
[29] section 2 (x) of the DPDP Act, 2023.
[30] As covered under chapter II

Data fiduciaries are accountable for adhering to the regulations[31] outlined in the 2023 Act, even when any data processing is carried out on their behalf by a data processor[32]. They are obligated to set up grievance redressal mechanisms16 to address complaints. Additionally, they must ensure the accuracy and completeness of personal information, especially when such data is used to make decisions impacting a user or when it is meant to be shared with another data fiduciary[33]. If a user withdraws their consent or if it's reasonable to assume that the original purpose is no longer relevant, such as in cases of prolonged user inactivity, data fiduciary must erase the data and ensure their data processors do the same. However, data can be retained by the data fiduciaries if mandated by law[34]. Unlike the 2022 Bill, which permitted data fiduciaries to retain data for unspecified "business and legal" reasons, this new legislation is more specific. Lastly, data fiduciaries are obligated to report instances of data breaches and give intimation to both the Data Protection Board (DPB) and the affected users.19

According to Section 6 (1) of the Act, Consent means an indication by the data principal signifying an agreement for their data to be processed for a specified purpose and be limited to such personal data as is necessary for such specified purpose. The consent given by the Data Principal shall be free, specific, informed, unconditional and unambiguous with a clear affirmative action. The 2023 Act limits the validity of consent to the personal data necessary for satisfying the specified purpose. Data principals also have the right to withdraw their consent20 and utilize the services of consent managers. For the purpose of this Act, Consent Manager[35] means a person registered with the Board, who acts as a single point of contact to enable a Data Principal to give, manage, review and withdraw her consent through an accessible, transparent and interoperable platform. In a situation where a Data Principal withdraws her consent to the processing of personal data under sub-section (5), the Data Fiduciary shall, within a reasonable time, cease and cause its Data Processors to cease processing the personal data of such Data Principal unless such processing without her consent is required or authorised under the provisions of the Act.

[31] As outlined under section 8 (1)
[32] "Data Processor" means any person who processes personal data on behalf of a Data Fiduciary as defined under section 2 (k)
[33] As outlined under section 8 (3)
[34] Sec 8 (7) Digital Personal Data Protection Act 2023
[35] Sec 2(g) Digital Personal Data Protection Act 2023

- **Rights and Duties[36] of Data Principal:**

The concept of 'data principal' has undergone a substantial expansion. It not only encompasses individuals but also includes parents or lawful guardians of children to whom the personal data pertains. Moreover, the definition has been extended to incorporate lawful guardians of 'persons with disabilities'.

While the term 'person with disability' lacks a precise explication within the DPDPB, it is notable that the Rights of Persons with Disabilities Act, 2016, forms the foundational legislation in India for recognizing the entitlements of individuals with disabilities. Under it, a 'person with disability' is defined as someone possessing enduring physical, mental, intellectual, or sensory impairments that, when compounded by societal barriers, impede their equitable participation in society, akin to their peers.[37]

Under the DPDP Act, certain rights of data principals may be highlighted: (i) Right to Information about Personal Data; (ii) Right to Correction and Erasure; (iii) Right of Grievance Redressal; and (iv) Right to Nominate. As such, data principals have the right to know a summary of the personal data processed, the identities of entities with whom their data has been shared, and the categories of personal data shared. Additionally, data principals can request correction, completion, updating, or erasure of their personal data processed by a data fiduciary.

The data fiduciary must make necessary corrections and updates. Erasure can be denied if retention is required by law. The DPDP Act also casts responsibility on the data principal to not impersonate another person or suppress information when applying for any document or proof from the state, and to provide only authentic information while exercising their right to data erasure.

Data principals shall have the right to have readily available means of grievance redressal provided by a data fiduciary in respect of any act or omission of such data fiduciary, regarding the performance of its obligations in relation to the personal data of such data principal or the exercise of her rights.[38] They can also nominate an individual to exercise their rights upon their death or incapacity.

[36] As covered under chapter III

[37] Section 2(s), The Rights of Persons with Disabilities Act, 2016.

[38] Section 13, Digital Personal Data Protection Act, 2023.

Individuals who are the subject of the data (referred to as data principals) have the right to request details about the personal data undergoing processing. This includes information about the processing operations being carried out and the identities of all the data fiduciaries and processors with whom their data has been disclosed. Data Principals also possess the authority to request data fiduciaries to rectify, complete, update or delete their personal information[39]. They retain the right to nominate an individual who can act on their behalf if they pass away or become incapacitated[40]. Data fiduciaries are obligated to establish easily accessible mechanisms for addressing complaints from data subjects. The 2023 legislation underscores the necessity for data principal to exhaust all available avenues for addressing grievances before involving the Data Protection Board (DPB). Moreover, the 2023 Act places the responsibility on data principal to refrain from impersonating others or withholding information while applying for any official documentation from the government. It further mandates that data principal provide accurate information when exercising their right to access data for correction and erasure.[41]

The Act upholds the definition of a 'child' as an individual below the age of 18 years, mirroring the definition from the 2022 Bill. Data fiduciaries are still required to secure 'verifiable[42]' parental consent for processing children's data. Furthermore, the Central Government holds the authority to grant exemptions to specific data fiduciaries from adhering to the obligation of obtaining parental consent. This can be achieved by lowering the age threshold for seeking parental consent, provided that the Central Government determines that the processing is being conducted in a manner that is demonstrably secure. In addition, it is mandatory for a data fiduciary to refrain from engaging in any processing of personal data that could potentially cause harm to the well-being of a child.

- **Data Protection Board of India**

According to the DPDP Act, the Data Protection Board (DPB) maintains its role as an entity responsible for adjudication and enforcement, rather than functioning as a regulatory

[39] 24 As regulated under section 12 (1)
[40] As regulated under section 14 (1)
[41] Duties of Data Principal as covered under section 15 of DPDP Act, 2023.
[42] DPDP Act does not define what ‘verifiable’ consent means.

body[43] . The central government retains authority over the structure and functioning of the DPB.[44] The 2023 Act offers comprehensive information regarding the composition[45] of the DPB and the prerequisites for membership, which were notably absent in the 2022 Bill. The Data Protection Board of India as established by the central government, will be tasked with essential functions that encompass several aspects. These functions[46] encompass:

(i) monitoring compliance and imposing penalties, (ii) directing data fiduciaries to take necessary measures in the event of a data breach, and (iii) hearing grievances made by affected persons.

The composition and manner along with terms of appointment of the Data Protection Board of India will be prescribed by the central government, which has raised questions on the independence of the board, which shall be discussed in greater detail, further in this article. It is envisioned as an Independent regulatory body responsible for monitoring and enforcing data protection laws. Its main role includes regulating and supervising data controllers, data processors, and other relevant entities, along with handling complaints and disputes related to data protection violations. Moreover, it is empowered to issue Orders and impose Penalties in cases of non-compliance with the Act's provisions, which can go up to 250 Crores, and varies, based on the nature and severity of the violation. The Act also mandates organizations to promptly notify the board and affected individuals in the event of a data breach. The order by the board can however be challenged in High Court in case of any dispute.

- **Penalties**

The DPDP can issue monetary penalties[47]to data fiduciaries in case of non-compliance. The newly introduced penalties under the DPDP involve potential fines reaching INR 250 Crores (two hundred and fifty million) for offenses, including the failure to implement reasonable security measures to prevent personal data breaches as outlined in Section 8(5) of the DPDPA. Importantly, the cap of INR 500 Crores (five hundred million) on penalties for a single instance has been removed, which means that data fiduciaries and processors

[43] As outlined under section 27
[44] As outlined under sections 16 & 17
[45] As outlined under section 19
[46] As outlined under section 27
[47] Section 33 of DPDP, 2023.

can now face higher penalties. It is worth noting that the right of a data principal to claim compensation for a breach of a data fiduciary's personal data protection obligations has been eliminated under the DPDPA

Furthermore, the DPDPA empowers the Board to impose a penalty of up to INR 10,000 (ten thousand) in cases where a data principal fails to fulfil their specified duties as outlined by the legislation. All sums realised by way of penalties imposed by the Board under this Act, shall be credited to the Consolidated Fund of India.[48]

Alternate Dispute Resolution: The provision for Alternate dispute resolution (ADR) is a progressive step for the addition of an efficient dispute resolution mechanism, which says that the board if it thinks fit, can direct this method to be adopted through mediation.

Progressive Legislation: The Act has used the pronouns 'she 'and 'her' as a way to express its positive support and promote women's empowerment. These were some of the highlight features by incorporation of which the legislation aims to ensure transparency, accountability, and individuals' control over their data while striking a delicate balance between the legitimate interests of organizations and the broader goal of technological progress and development.

3.4 CRITICAL ANALYSIS OF THE ACT

The Digital Personal Data Protection Act (DPDPA) 2023 marks a significant step forward for India in establishing a robust legal framework for personal data protection. While the Act may have limitations in its application to specific areas like wearable technology (addressed in Chapter 4), it offers several strengths that enhance data privacy for individuals across the nation.

- **Emphasis on User Consent:**

The DPDPA prioritizes informed consent as the cornerstone of data collection and processing. It mandates that data fiduciaries (entities handling personal data) obtain clear and unambiguous consent from individuals before processing their data. This consent must

[48] Section 34 of DPDP Act 2023

be freely given and specific to the purpose of data collection. Users have the right to withdraw consent at any time, ensuring ongoing control over their data.

The Act's strength lies in its focus on informed consent. Data fiduciaries are obligated to provide users with transparent information about the data collected, the purpose of processing, and how the data will be used. This empowers individuals to make informed decisions about sharing their personal information. Additionally, the Act prohibits unfair terms within consent agreements, preventing companies from manipulating users into giving blanket consent.

- **Data Minimization and Purpose Limitation:**

The DPDPA emphasizes the principle of data minimization. This principle dictates that data fiduciaries can only collect personal data that is necessary for a specific, clearly defined purpose. Additionally, data can only be processed for the purpose it was collected for, preventing unauthorized use or secondary purposes without further consent.

This provision strengthens data privacy by limiting the amount of personal information collected and stored. It prevents data fiduciaries from amassing vast troves of unnecessary data, reducing the potential for misuse or data breaches.

- **Data Breach Notification:**

The DPDPA mandates data fiduciaries to notify individuals and the Data Protection Board (DPB) in case of a data breach. The Act defines a data breach as an unauthorized access to or disclosure of personal data that poses a risk of harm to individuals. The notification timelines are crucial - the Act mandates reporting breaches within a specific timeframe, allowing for timely intervention and mitigation strategies.

This provision is critical for data security and empowers individuals to take action to protect themselves. By being notified of a data breach, users can change passwords, monitor financial statements for fraudulent activity, and take steps to minimize potential harm. Additionally, the requirement to report breaches to the DPB allows for regulatory oversight and enforcement actions against data fiduciaries who fail to comply with data security standards.

- **Rights of Data Principals:**

The DPDPA empowers individuals, known as data principals, with a range of rights regarding their personal data. These rights include:

- **Right to access:** Individuals have the right to request access to their personal data held by a data fiduciary. This allows them to verify the accuracy of the data and understand how it is being used.
- **Right to rectification:** Data principals can request correction of any inaccurate or incomplete personal data.
- **Right to erasure:** Individuals have the right to request the erasure of their personal data under certain circumstances, such as when it is no longer necessary for the purpose for which it was collected.
- **Right to restrict processing:** Data principals can restrict the processing of their personal data in specific situations.
- **Right to data portability:** Individuals have the right to obtain their personal data from a data fiduciary in a machine-readable format and transfer it to another data fiduciary.

These rights grant significant control to individuals over their personal data. They can access, rectify, or erase their data, ensuring its accuracy and preventing unauthorized use. Additionally, data portability allows for greater control over one's digital footprint, fostering competition among data fiduciaries and potentially encouraging better data privacy practices.

- **Grievance Redressal Mechanism:**

The DPDPA establishes a grievance redressal mechanism for individuals to address their concerns regarding data protection violations. They can file complaints with the DPB, which is empowered to investigate and issue appropriate orders against data fiduciaries. This mechanism provides individuals with an avenue to seek recourse for data privacy violations and ensures accountability from data fiduciaries.

3.5 CONCLUSION

The discussion demonstrate the DPDPA's potential to create a more robustdigital data privacy landscape in India.The Act emphasizes simplicity in language and structure, presenting

definitions such as Data fiduciary and Data principal to foster a clear understanding of its provisions, despite the technical nature of the subject. It extends its scope to digital personal data handling within India and sets limitations on data processing outside India unless it is for providing services or goods within the country. Significant Data Fiduciaries are introduced, highlighting the Act's focus on safeguarding sensitive data through measures like audits and data protection impact assessments. Consent is crucial, as indicated in Section 6 (1), requiring it to be free, specific, informed, and unambiguous, with provisions for data principals to manage or withdraw their consent via a Consent Manager. Data Principal under the DPDP Act, including rights such as information, correction, grievance redressal, and nomination. It emphasizes the inclusion of parents or guardians for children and those with disabilities as data principals. The legislation mandates data fiduciaries to ensure transparency and accountability in data processing, along with establishing grievance redressal mechanisms. Additionally, it touches upon the responsibilities of data principals and the role of the Data Protection Board in India, underscoring the importance of personal data protection.

The Act emphasis on user consent, data minimization, and purpose limitation to enhance privacy. It introduces steep monetary penalties for data fiduciaries and processors for non-compliance and the failure to implement adequate security measures against data breaches. With the removal of a cap on penalties and the elimination of a data principal's right to claim compensation, the legislation aims to enforce strict compliance while also taking a progressive step through the inclusion of an alternate dispute resolution mechanism. The DPDPA provides individuals, or data principals, with comprehensive control over their personal data through various rights such as access, rectification, erasure, restriction of processing, and data portability. Additionally, it establishes a grievance redressal mechanism, empowering individuals to address complaints about data protection violations directly to the DPA, thereby ensuring accountability and encouraging better data privacy practices among data fiduciaries. . It is important to acknowledge that the Act is relatively new, and its effectiveness will depend on strong implementation and enforcement mechanisms. Additionally, as discussed in Chapter 4, certain aspects of the Act may need further refinement to effectively address the unique challenges of data collection in the context of wearable technology.

CHAPTER 4

DPDP ACT AND GAPS IN WEARABLE TECH DATA PROTECTION

4.1 INTRODUCTION

As we transition into a more technologically integrated era, as we discussed in Chapter 3, the Digital Personal Data Protection Act (DPDPA) 2023, which aims to regulate the collection, storage, and usage of personal data, represents a pivotal attempt by the Indian legislature to address the burgeoning concerns surrounding data privacy. Wearable devices, capable of tracking personal information from health metrics to geographical location, pose unique challenges that necessitate robust regulatory frameworks. This chapter aims to dissect the intricacies of the DPDPA 2023, shedding light on its attempts to safeguard user privacy and the areas where the Act might fall short in the face of the rapid evolution of wearable gadgets.

The exploration begins with a detailed examination of the statute's provisions related to wearable technology. This includes an analysis of the Act's scope concerning data collected by wearables, the consent mechanism for data processing, and the rights conferred upon individuals regarding their information. Following this groundwork, the chapter delves into a critical evaluation of the DPDPA 2023, pinpointing the gaps that emerge when the Act is juxtaposed against the technological realities of wearables. Particular attention will be devoted to identifying the loopholes that could potentially be exploited to undermine data privacy. This encompasses a discussion on the sufficiency of consent in the era of pervasive data collection, the Act's applicability to international entities dealing with Indian users' data, and the enforcement mechanisms available to uphold the rights enshrined in the law.

4.2 SENSITIVE DATA

The Digital Personal Data Protection Act (DPDP) Act 2023 has been criticized for not explicitly categorizing certain types of data as "sensitive" and affording them stronger protections. This is particularly relevant to health information collected by wearable technology devices. This lack of specific categorization in the DPDP Act can hinder wearable device data protection by drawing a lower protection standard.

- **Lower Protection Standard:** The Act classifies data broadly, without distinguishing between "personal data" and "sensitive personal data" like health information. This means health data from wearables might not receive the same level of protection as financial data. In general, while personal information obviously includes an individual's personal details, such details need not always be considered 'sensitive'. Although informational 'sensitivity' is one of the prescribed evaluative parameters in respect of (Significant Data Fiduciary) SDF notifications[49] under Digital Personal Data Protection Act 2023, the only allusion to sensitivity that DPDP's present-day draft makes is under Section 10: "The Central Government may notify any Data Fiduciary or class of Data Fiduciaries as Significant Data Fiduciary, on the basis of an assessment of such relevant factors as it may determine, including— (a) the volume and sensitivity of personal data processed", which in turn spells out additional obligations of SDFs). Moreover, DPDPA does *not* explicitly define or refer to sensitive personal data or information ("**SPDI**") either. Nevertheless, the Central Government can notify any data fiduciary as an SDF based on the assessment of sensitivity with respect to personal data processed by the data fiduciary.[50]

- **Limited User Controle:** Since the DPDP Act doesn't categorise health data from wearables as sensitive, users might have less control over who can access and use this information. This could lead to situations where users are unaware of how their health data is being shared or sold to third parties. Our analysis reveals that the DPDP Act's broad data classification approach, which doesn't distinguish between 'personal data' and 'sensitive personal data' like health information collected by wearables, creates a weaker protection standard compared to the GDPR's tiered classification system. This can lead to scenarios where users have less control over how their sensitive health data is collected, used, and shared by wearable tech companies. For instance, under the DPDP Act, a company developing a fitness tracker app might collect a user's sleep data and argue that it falls under the umbrella of 'personal data' for 'personalized coaching.' However, this data could also be

[49] The Central Government may notify any data fiduciary as an SDF based on the assessment of relevant factors such as the volume and sensitivity of personal data processed, risk to the rights of data principal and the potential impact on the integrity of India.

[50] Deborshi Barat, "Sense and Sensitivity : 'Sensitive' Information Under India's New Data Regime," S&R Associates, December 22, 2023, https://www.snrlaw.in/sense-and-sensitivity-sensitive-information-under-indias-new-data-regime/.

> used for targeted advertising without explicit user consent, which wouldn't be permissible under the GDPR's stricter classification for sensitive health data."[51]

While the DPDP Act recognises that additional processing requirements are necessary for certain categories of data principals like children and people with disabilities under Section 9, it does not contain any provisions for special categories of data. Before the enactment of the DPDP Act, sensitive personal data like medical, health and biometric data was regulated by the IT Rules. The IT Rules 2011 provided that the collection of 'sensitive personal data or information' is to be subject to enhanced rules such as explicit consent in writing through letter or fax or email. The IT Act provided for compensation for negligence in implementing and maintaining 'reasonable security practices and procedure' for processing sensitive data or information under Section 43A and provided for punishment for disclosure of personal information under Section 72A. Corresponding protections and provisions are conspicuous by their absence under the DPDP regime. It is pertinent to note that both the Personal Data Protection Bill, 2019 and the recommendations of the Joint Parliamentary Committee provided for added protections for special category of data i.e. sensitive data. Unfortunately, under the DPDP regime, sensitive personal data like personal health data, biometrics, financial data, etc. has been placed on the same pedestal as personal data like email, postal address, phone number etc. Section 6 of the DPDP Act, which requires data principals to provide consent that is "free, specific, informed, unconditional and unambiguous", also does not provide an enhanced threshold for more sensitive categories of data.

It is also germane to note that even though Section 10 of the DPDP Act allows the Central Government to notify any data fiduciary or class of data fiduciaries as 'significant data fiduciary' on the basis of certain factors, one of them being the 'sensitivity of the data processed', if the data fiduciary processing 'sensitive data' like health records, biometrics, financial information, etc. can be given special status, why did the legislature stop short of defining sensitive data or not accord it any special status? The answer may be that all personal data could become sensitive personal data. Sometimes, various data points that, when separately processed, are considered to be non-sensitive; however, when they are combined in certain combinations and then processed, they may be considered to be sensitive and may result

[51] "India's Digital Personal Data Protection Act 2023 vs. the GDPR: A Comparison," India's Digital Personal Data Protection Act 2023 Vs. The GDPR: A Comparison, November 2023, https://www.lw.com/admin/upload/SiteAttachments/Indias-Digital-Personal-Data-Protection-Act-2023-vs-the-GDPR-A-Comparison.pdf.

in significant privacy violations and harms. Here's an illustrative example to consider: separately, a dataset that includes individuals' restaurant check-ins on social media may be regarded as non-sensitive. Similarly, a dataset with anonymous health records might not be seen as sensitive if there's no way to identify individuals. However, if these two datasets are combined, it might be possible to infer sensitive health conditions of specific individuals based on their eating habits and locations they frequent, thus creating potential privacy violations and harms. This scenario demonstrates how seemingly non-sensitive data, when aggregated, can become sensitive and pose risks to individual privacy. However, even this explanation does not take away from the certitude that, data which at the very outset is sensitive personal data needs to be accorded a special status and added protections.

As highlighted earlier, the lack of specific protections for sensitive health data collected by wearables in the DPDP Act can play out in many ways, for instance; Wearable data can be anonymized and sold to data aggregators, who might then be able to re-identify individuals, especially when combined with other datasets. sensitive health data collected by wearables in the DPDP Act opens the door for potential misuse by companies and even the government. Companies, particularly insurance firms, could leverage health data from wearables to discriminate against individuals. For instance, data on pre-existing health conditions derived from activity trackers might lead to higher insurance premiums or even denials for coverage. Detailed health information, like sleep patterns or dietary habits, could be used for highly targeted advertising. This could be intrusive and manipulative, especially for individuals with specific health concerns. Companies might share or sell anonymized wearable health data to third parties, such as data brokers or research institutions. While anonymized, this data can sometimes be re-identified, especially when combined with other datasets, posing privacy risks for individuals. Governments could access wearable health data for surveillance purposes, raising concerns about potential misuse and limitations on individual freedoms. While government access to anonymized health data could benefit public health initiatives, the lack of clear regulations in the DPDP Act raises concerns about potential mission creep. Law enforcement agencies could seek access to wearable health data in criminal investigations. Without clear legal frameworks and judicial oversight, this access could infringe upon individual privacy rights.

The DPDP Act does have provisions for user consent and data security. However, the lack of specific categorization for sensitive health data weakens these protections when it comes to

wearable technology. This can lead to a loss of user control, potential exploitation for commercial gain, and even limitations on individual freedoms.

4.2 LEGITIMATE PURPOSE

The Act's "legitimate purpose" clause is not be clear enough for informed consent regarding wearable data collection. Informed consent means agreement or permission to do something from someone who has been given full information about the possible effects or results.[52] The "legitimate purpose" clause in the DPDP Act 2023 is intended to strike a balance between allowing businesses to collect and use data for legitimate purposes and protecting user privacy. However, this clause can be problematic when it comes to informed consent for wearable data collection, due to several reasons:

- **Ambiguity in "Legitimate Purpose":** The Act doesn't clearly define "legitimate purpose." This ambiguity creates uncertainty for both businesses and users. Companies might interpret " legitimate purpose" quite broadly, collecting more data than what's strictly necessary for the stated purpose. For instance, a fitness tracker app might collect sleep data under the guise of offering "personalized coaching," but this data could also be used for targeted advertising. The DPDP Act, through Section 4, allows processing of personal data only after the requirement for consent under Section 6 have been fulfilled, or for the ‘legitimate uses’ mentioned under Section 7. However, under Section 7(f) and 7(g), a data fiduciary can process personal data for responding to medical emergency involving threat to life or health of data principal or any other person and for taking measures to provide medical treatment or health services during an epidemic, outbreak, disease or any other threat to public health respectively. It is pertinent to note that in the above circumstances the data principal would reasonably not be in a position to provide consent that would fulfil the requirements of Section 6; therefore, this consent can be considered to be at best deemed. This concept of consent along with the absence of mitigating measures for harm as well as risk regulation measures under the DPDP regime may limit the autonomy of an individual over their health data.

[52] Merriam-Webster. (2022). Definition of "informed consent." In *Merriam-Webster.com*. https://www.merriam-webster.com/dictionary/citation

- **Limited User Control**, when consent isn't truly informed, users have less control over their wearable data. They might be unaware of the extent of data collection and how it's being used.
- **Privacy Risk**: Unclear "legitimate purpose" and bundled consent[53] can lead to situations where users unknowingly give away more data than they intended.
- **Trust Concern**: This can increase the risk of data breaches, misuse, and even identity theft. If users feel they can't make informed decisions about their wearable data, it can erode trust in the wearable tech industry and hinder its growth.

4.3 PRE-CHECKED CONSENT BOXES

The DPDP Act's reliance on consent for wearable data collection can be undermined by practices like pre-checked consent boxes and bundled service agreements. the concept of informed consent is fundamentally challenged in the digital age. Applications in wearable devices are often characterized by information overload, complex terms of service, and pre-checked consent boxes. This creates a situation where users struggle to understand what data they are consenting to and how it will be used. This lack of meaningful consent is particularly concerning in the context of wearable technology data collection, where continuous streams of sensitive health information are involved. For example, a fitness tracker app might present a single, pre-checked consent box requesting permission to 'collect all user data for personalized experience.' This vague language fails to inform users about the specific data points being collected (sleep patterns, heart rate, location) or how this data might be used beyond personalized workout recommendations. In such scenarios, users are pressured to accept bundled service agreements or pre-checked consent options to utilize the wearable technology, even if they're uncomfortable with the amount of data being collected or the potential for its secondary use."[54]

- **All-or-Nothing Choice:** Pre-checked consent boxes present users with a binary choice: accept all data collection practices or forgo using the wearable altogether. This doesn't provide a genuine opportunity for informed consent, especially when dealing with

[53] Bundled consent refers to the practice of 'bundling' together multiple requests for an individual's consent to a wide range of collections, uses and disclosures of personal information, without giving the individual the opportunity to choose which collections, uses and disclosures they agree to and which they do not.
[54] Daniel J. Solove, The Digital Person: Technology and Privacy in the Information Age, 2004, https://ssrn.com/abstract=2899131.

continuous data streams. Wearable data can be incredibly detailed, encompassing sleep patterns, location every few minutes, heart rate, and activity levels. A user might be comfortable with the wearable tracking basic steps, but uncomfortable with constant location tracking or sleep monitoring. With a pre-checked box, they can't opt-out of specific data collections.

- **Lack of Transparency:** Pre-checked boxes often obscure the details of what data is being collected and how it's being used. Users might be unaware of the extent of data collection, making it difficult to give meaningful consent. Imagine a scenario where a pre-checked consent box for a fitness tracker app simply states "data will be used to personalize your experience." This vague statement doesn't inform the user that their sleep data might be sold to a third-party for targeted advertising.

- **Undue Pressure:** Pre-checked boxes can create pressure on users to simply accept the terms and conditions without careful consideration. This is especially true if the user has already invested in the wearable device or is eager to start using a new fitness app.

- **Informed Consent:** Informed consent typically takes the form of asking users to agree to privacy policies which specify what information will be recorded and in what ways it will be used. These privacy policies are long documents which exhaustively list all the ways in which the personal data might be used. The problem with this “notice and consent” approach to privacy lies in the fact that very few people read privacy statements. Furthermore, there is abundant evidence that even the few people who do read privacy policies do not understand them[55]. Ticking boxes under long and incomprehensible privacy policies does not constitute informed consent. The think tank Brookings points out that while “the shortcomings of consent are often acknowledged, the response is often a push for more and better consent”[56]. Clearly, longer and more thorough privacy policies are not the answer. One of the most widely discussed alternatives to the “notice and consent”

[55] Yannis Bakos & Florencia Marotta-Wurgler & David R. Trossen, 2009. "Does Anyone Read the Fine Print? Testing a Law and Economics Approach to Standard Form Contracts," Working Papers 09-04, NET Institute, revised Aug 2009

[56] David Medine and Gayatri Murthy, “Companies, not people, should bear the burden of protecting data,” Brookings, December 18, 2019, https://www.brookings.edu/articles/companies-not-people-should-bear-the-burden-of-protecting-data/.

approach is shifting the focus from the collection of personal data to its usage [57]. This puts the burden on companies, rather than individuals, to protect privacy. Wearable device manufacturing companies should be restricted to using user data for "legitimate purposes consistent with reasonable expectations formed in their relationships with users." However, for uses of personal data outside of these reasonable expectations, informed consent is still required. The question then becomes, 'which actions require informed consent, and which do not?' Addressing this issue in the context of healthcare, [58] informed consent should be understood with reference to a background of social norms, ethical standards and legal obligations. By asking users to consent to an exhaustive list of all the different ways their personal data might be used, the real privacy issues at stake are drowned out by irrelevant detail. For example, consider the following excerpts from the privacy policies of Facebook, Google, and Snap (formerly Snapchat) Inc. respectively, when you use Messenger or Instagram to communicate with people or businesses, those people and businesses can see the content you send[59] if you contact Google, they'll keep a record of your request in order to help solve any issues you might be facing.[60]When you interact with their services, they collect information that you provide to them.[61] The listing of such details leads to lengthy privacy policies that are difficult to understand, even for users who are intent on reading them. As it recommended above that if consent only applies to uses of information that deviate from expected social norms, privacy policies would be drastically shortened and would focus on the real issues that individuals are consenting to. This leaves open the question of specifying what the norms are.the government should determine and specify the norms of information usage. In the UK, the Information Commissioner's Office (ICO, an independent public body sponsored by the Department for Digital, Culture, Media & Sport) is tasked with offering guidance, advice and promoting good practice for data protection. They could compile a list of social norms and expected behaviours to serve as a standard against which privacy policies can be formulated. The UK government already uses this approach within the context of healthcare – the National Data Guardian (sponsored by the Department of Health and Social Care) provides guidelines as to what constitutes a

[57] F. H. Cate and V. Mayer-Schonberger, "Notice and consent in a world of Big Data," International Data Privacy Law 3, no. 2 (May 1, 2013): 67–73, https://doi.org/10.1093/idpl/ipt005.
[58] Neil C. Manson and Onora O'Neill, Rethinking Informed Consent in Bioethics, 2007, https://doi.org/10.1017/cbo9780511814600.
[59] Facebook, "Data policy," April 2018. [Online]. Available: https://www.facebook.com/ policy.php
[60] Google, "Privacy policy," March 2020. [Online]. Available: https://policies.google.com/ privacy
[61] S. Inc., "Privacy policy," December 2019. [Online]. Available: https://www.snap.com/ en-US/privacy/privacy-policy

"reasonable expectation" when sharing healthcare data[62]. Similar regulations needs to be brought under dpdpa These guidelines can be extended into other domains relevant to privacy. The burden then lies with each company or organisation seeking the consent of its users to explain the ways in which their use of personal information deviates from the guidelines set out by these public bodies. This will alleviate the problem of long and incomprehensible privacy policies while ensuring that users are informed and are able to give consent. Although the line between reasonable and unreasonable cannot be sharply defined, an attempt must be made. Disagreements that arise from this (necessarily) vague definition can be solved through the justice system.[63]

- **Withdrawal of Consent:** Since consent forms not only the basis of the data privacy and protection but is a non-negotiable aspect thereof, therefore, the right to withdraw consent is also an essential aspect as it also flows from the right to privacy and self-determination. The DPDP regime provides the data principal the right to withdraw his/her consent at any time and with the same ease as that was present for giving the consent under Section 6(4). However, there is an obstacle to this right, under Section 6(6) whereby the data fiduciary is allowed to process the personal data of the data principal even after the withdrawal of consent for a 'reasonable time'. The regime does not specify a maximum period for reasonable time nor does it provide who decides how long the period should be and on what basis should this time be decided. This latitude under the DPDP Act leaves the data principal in a perilous position as his/her data is being processed and may continue to be processed without consent for a 'reasonable period of time' that is neither to his/her knowledge nor control.
- **deletion of data** : Another corresponding right to the right of withdrawal of consent, is the right of erasure/deletion of data post the withdrawal of consent. While Section 12(3) does allow the data principal the right to ask for erasure of his/her personal data, this right also faces the same encumbrances like the right to withdraw consent. It also does not provide any timeline for erasure and is even qualified as it allows the data fiduciary to retain the personal data if the same is 'necessary for the specified purpose or for the compliance of any law'. Consequently, leaving the data principal again with just a right in name. It is

[62] F. H. Cate and V. Mayer-Schonberger, "Notice and consent in a world of Big Data," International Data Privacy Law 3, no. 2 (May 1, 2013): 67–73, https://doi.org/10.1093/idpl/ipt005.
[63] Anna Bruvere and Victor Lovic, "Rethinking Informed Consent in the Context of Big Data," April 19, 2021, https://doi.org/10.17863/cam.68396.

pertinent to note that Article 17 of the EU GDPR as well as the UK GDPR provides for the right to erasure post the withdrawal of consent ‘without any undue delay’.

4.4 BUNDLED SERVICE AGREEMENTS

Bundling data collection practices with core functionalities of the wearable or app can coerce users into consenting to more data collection than they might prefer. For instance, imagine a wearable that requires users to agree to data sharing with third-party advertisers to unlock features like workout plans or personalized coaching. This limits user options and makes it difficult to separate core functionalities from data collection practices.Bundled service agreements can mask the true cost of using a wearable. While the wearable itself might be inexpensive, the bundled agreement might require users to give away valuable personal health data in exchange for using all the features.Service agreements are often lengthy and complex legal documents. The average user might not have the time or expertise to negotiate the terms, especially when bundled with core functionalities of the wearable.In such caes users might not be aware of the data being collected or how it's being used, creating privacy risks.Users have less control over their wearable data and cannot make granular choices about what data is collected.

The regulation should require manufacturers to provide clear and easily understandable information about data collection practices and purposes. This information should be separate from other terms of service and presented in a way that users can easily access and comprehend. It is necessary to Mandate that users are informed upfront about any data sharing with third-party advertisers or other entities as part of bundled agreements. This ensures users are fully aware of what they are consenting to before using the wearable's core functionalities.

4.5 UNCERTAINTIES AROUND ANONYMIZED DATA:

- **Silence on Anonymization:** The Act doesn't address anonymized data, which can sometimes be de-anonymized, especially when combined with other datasets.The Act doesn't explicitly address anonymized data. It focuses on protecting "personal data" that can be directly linked to an individual. This lack of clear regulation for anonymized data creates a grey area.
- **Risk of Re-identification:** While anonymization techniques remove identifiers like names or addresses, data can sometimes be re-identified, especially when combined with other

datasets. For instance, anonymized location data from a wearable might be seemingly harmless on its own. However, when combined with a publicly available social media post mentioning your location at a specific time, it could potentially be used to re-identify you. The growing popularity of wearable technology devices has raised concerns about the privacy of the data they collect, particularly health information. While anonymization techniques are often used to protect user privacy, these techniques may not be sufficient in the age of big data. the anonymized data from wearables, especially when combined with other datasets, can be re-identified with surprising ease. For instance, anonymized location data from a wearable might include timestamps and show frequent visits to a specific gym. If a user publicly shares on social media that they frequent a particular gym at a certain time, this seemingly anonymized data can be linked back to the individual. This re-identification risk poses a significant threat to user privacy, as it can expose sensitive health information and lead to discriminatory practices, such as denying insurance coverage based on inferred health conditions.[64]

- **Reduced Privacy Protections:** Since anonymized data falls outside the Act's purview, companies might handle it with less care, potentially leading to situations where it's used for unintended purposes or even sold to third parties. Computer scientists have recently undermined our faith in the privacy-protecting power of anonymization, the name for techniques for protecting the privacy of individuals in large databases by deleting information like names and social security numbers. These scientists have demonstrated they can often 'reidentify' or 'deanonymize' individuals hidden in anonymized data with astonishing ease. By understanding this research, we will realize we have made a mistake, labored beneath a fundamental misunderstanding, which has assured us much less privacy than we have assumed. This mistake pervades nearly every information privacy law, regulation, and debate, yet regulators and legal scholars have paid it scant attention.[65]

- **Increased Risk of Discrimination**: Even anonymized data can be used for discriminatory practices. For instance, anonymized health data from wearables could be used to create risk

[64] Anglano & C. Lipman (2022). When Anonymized Isn't Enough: Re-identification Risks in the Age of Wearable Technology. Santa Clara Law Review, 59(2), 521-558.
[65] Paul Ohm, “BROKEN PROMISES OF PRIVACY: RESPONDING TO THE SURPRISING FAILURE OF ANONYMIZATION,” 57 UCLA LAW REVIEW, 2010, https://www.uclalawreview.org/pdf/57-6-3.pdf.

profiles for insurance purposes, potentially leading to higher premiums or even denials for coverage for certain demographics.

- **Chilling Effect on Innovation:** The uncertainty surrounding anonymized data can discourage companies from investing in innovative data-driven solutions that utilize anonymized datasets for research or public health initiatives.

4.6 LOCATION DATA CONCERNS

The privacy risks this poses for users of wearable tech is high, especially when health or location data is involved. When the DPDP Act doesn't effectively address anonymized data, it creates significant privacy risks for users of wearable technology, particularly when dealing with sensitive information like health or location data. Since the law doesn't explicitly exclude or include anonymized data. If data is irreversibly anonymized and cannot be used, even with other information, to identify a person, it likely wouldn't be covered by the DPDP Act.

Anonymized data, especially health or location data, can sometimes be re-identified, particularly when combined with other datasets. This can happen through techniques like matching anonymized data points with publicly available information on social media or other sources. Once re-identified, this data can be used to track individuals, create detailed profiles, or even expose sensitive location information.If health data from wearables, even when anonymized, can be re-identified, it exposes users to a range of privacy risks.Even anonymized health data can be valuable for targeted advertising..Re-identified location data, combined with other personal information, can be used for identity theft purposes. This could lead to financial losses or even damage an individual's reputation.

- **Privacy Violations:** Wearables often collect location data, which can be very revealing. Even anonymised location data can paint a picture of an individual's routines, habits, and frequented locations. This can be a privacy violation, especially if the data falls into the wrong hands.
- **Stalking and Safety Risks:** In extreme cases, re-identified location data from wearables could be used for stalking or other malicious purposes. This can pose a significant safety risk for users, particularly vulnerable individuals. Imagine someone using a wearable that tracks sleep patterns. This data is anonymised and sold to a research institution. However, when combined with the individual's social media posts mentioning their sleep schedule, the data becomes identifiable. This could expose their health information and potentially

lead to discrimination by insurance companies. In another scenario, anonymised location data from a wearable is used to create a heatmap of user activity in a specific city. While anonymised, this data can be combined with other sources to identify frequently visited locations of a particular individual, potentially compromising their privacy and safety.

The DPDP Act's shortcomings regarding anonymised data leave users of wearable technology vulnerable to privacy risks, especially when dealing with sensitive health or location information. By implementing stricter regulations for anonymized data and promoting user awareness, these risks can be mitigated, fostering a more secure and privacy-conscious environment for the wearable tech industry.

4.7 LACK OF SECURITY AUDITING MANDATE

To address the growing concerns surrounding data protection and privacy in wearable technology, it is essential to include a security auditing mandate specifically for this sector in the Digital Personal Data Protection Act. This mandate should make it mandatory for organisations dealing with wearable technology to undergo regular security audits conducted by certified third-party vendors.

By incorporating a security auditing mandate, the government can ensure that organisations implementing wearable technology prioritise the protection of sensitive data. The audits would reveal any gaps or weaknesses in the existing security controls, enabling organisations to take corrective measures. Non-compliance with the security auditing mandate should attract penalties, thereby creating a strong incentive for organisations to prioritise data protection. Furthermore, the requirement to submit the audit reports to a government-appointed board would ensure transparency and accountability. This board could assess the audit reports, provide recommendations, and monitor the implementation of necessary security measures, thereby strengthening the overall data protection ecosystem in India.

A security audit is a regular test to see if the company actually has the controls to secure the sensitive data. These audits reveal the gaps and lapses which can lead to leakage of data.As per the DPDPA, it is left to the organizations to choose whether to have an audit or not. As an analogy, it is like saying the companies can themselves ensure they are paying the taxes, there is no need for audits. Having a law that is prepared in 2023, much later than most of the nations in the world, it was essential to make it necessary for certain sectors like Fintech, Healthcare

and some crucial sectors that are storing sensitive data like health records, financial records etc. to have regular security audits by certified third party vendors and submit the report to the board created by the government.

Countries like the USA, Singapore, UAE, and even smaller nations like Oman have policies for regular third-party security audits of companies in specific sectors, yet India is still far from this race. To note that there is a mention of audits for organisations which only the Central Government recommends based on certain factors like data related to national safety/public order. Auditing of a database must be done on a periodic basis. There are three main reasons for this. Firstly, periodical assessment can mitigate the risks introduced by the database system. Secondly, the efficiency of controls relating to the database can be evaluated, and finally, the audit review can help to continually improve the internal processes, procedures and tools, thus, the overall effectiveness and efficiency of the database system implemented.[66]

4.8 LIMITED RIGHT TO DATA PORTABILITY

Two crucial omissions stand out the right to data portability and the right to be forgotten. The Act does not provide these basic rights which have been backed up as strong rights in landmark cases[67]The right to data portability empowers individuals, referred to as data principals, to obtain and transfer their personal data from data fiduciaries (companies collecting the data) in a readily usable format. This right is particularly relevant in the context of wearable technology. Imagine a scenario where you've been using a fitness tracker for years, meticulously logging your health data. Suddenly, you decide to switch to a different brand or service. Without data portability, you'd risk losing years of valuable information. This right ensures continuity and empowers users to choose service providers that best suit their needs, fostering competition and innovation in the wearable tech market.

The absence of the right to be forgotten creates an even greater concern. Wearable technology collects a vast amount of personal data, from location history and sleep patterns to health metrics and activity levels. Over time, this data profile may contain elements an individual no

[66] Muneeb -Ul-Hasan and Siti Hajar Othman, "A Conceptual Framework of Information Security Database Audit and Assessment," International Journal of Innovative Computing 9, no. 1 (May 31, 2019), https://doi.org/10.11113/ijic.v9n1.206.

[67] Mukhija, Khilansha, and Shreyas Jaiswal. "Digital Personal Data Protection Act 2023 in light of the European Union's GDPR." Jus Corpus Law Journal, November 7, 2023, 638-649.

longer wants to be associated with them. Perhaps a past health condition or location data from a sensitive period needs to be erased. The right to be forgotten empowers users to request the deletion of their data, fostering a sense of control over their digital footprint. This right is critical for ensuring individuals can evolve beyond their data and potentially make amends for past actions reflected in their digital history. The DPDP Act's lack of these fundamental rights weakens its ability to safeguard user privacy. Imagine a scenario where a wearable tech company experiences a data breach, exposing sensitive information about millions of users. Without the right to be forgotten, individuals may have limited recourse to remove this compromised data from circulation. Similarly, a lack of data portability restricts users' ability to easily migrate their data to a more secure platform after such a breach.

4.9 AUTOMATED DATA AND DIGITISED DATA

The DPDP Act of 2023 introduces a potential blind spot in data security for wearable technology users due to ambiguity regarding "automated data" vs. "digitised data." The Act clarifies that offline data falls under its protection only when digitised. This, however, creates a loophole that might exclude a significant portion of the data collected by wearables - automated data. Wearable technology continuously generates a stream of personal data, including sensitive information like health metrics (heart rate, sleep patterns), location history, and potentially even biometric data. This data stream, often categorised as "automated data," might not be fully covered by the DPDP Act due to ambiguity surrounding its definition.[68] Even if it is, the unrestricted transfer of this sensitive data to countries with lax data protection laws creates a significant security risk.

Imagine a smartwatch that constantly monitors your heart rate. This real-time data, crucial for fitness tracking, wouldn't be covered by the Act until it's stored on a device or app (digitized). This ambiguity raises concerns. Firstly, it weakens data protection for users. Automated data collected by wearables can be highly sensitive (health metrics, location history). Leaving it unregulated creates a vulnerability for potential misuse. Secondly, the real-time nature of automated data adds another layer of complexity. While digitized data might be a static

[68] Cynthia Jayapal et al., “Challenges in Wearable Technology,” 2021 International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA), October 8, 2021, https://doi.org/10.1109/icaeca52838.2021.9675758.

snapshot, automated data is constantly generated, raising questions about when and how the Act applies its protections.

A significant portion of wearable data, specifically automated data, might be excluded. This ambiguity raises concerns as automated data collected by wearables can be highly sensitive, encompassing health metrics, location history, and biometric information.[69]Leaving such data unregulated weakens user privacy protection. Additionally, the real-time nature of automated data adds another layer of complexity. While digitized data might be a static snapshot in time, automated data is constantly generated, raising questions about when and how the Act applies its protections. Instead of the previously proposed Independent Authority, the Act has come up with the provision for setting up the Data Protection Board of India, but there have been a lot of debates on the independence of the board, which has now been referred to as a mere controlling tool in hands of the central government, as the government has been empowered in regards to the constitution and functioning of the board, along with other provisions. Hence, there have been a lot of concerns about this blanket power to the central government giving a Surveillance state tint to it.

4.10 DATA TRANSFER

The Digital Personal Data Protection Act (DPDP) of 2023, while aiming to regulate data privacy in India, presents a potential security concern for wearable technology users regarding cross-border data transfers. Unlike the European Union's General Data Protection Regulation (GDPR) with its stringent regulations, the DPDP Act offers a more relaxed approach. The GDPR mandates specific conditions for transferring personal data outside the EU, such as ensuring the receiving country has adequate data protection laws ("adequacy decisions"). In contrast, the DPDP Act allows for freer data transfers, with restrictions only applicable to countries on a "negative list" designated by the Central Government. This raises concerns for wearable tech users due to the nature of data collected by these devices.

[69] Khan, Saad, Simon Parkinson, Liam Grant, Na Liu, and Stephen Mcguire. “Biometric Systems Utilising Health Data from Wearable Devices.” ACM Computing Surveys 53, no. 4 (July 11, 2020): 1–29. https://doi.org/10.1145/3400030.

4.10 CONCLUSION

In conclusion, the Digital Personal Data Protection Act (DPDP) Act 2023 marks a significant step towards enhancing data privacy and security in India, especially in the context of wearable technology. However, the Act exhibits notable gaps in its framework; the Digital Personal Data Protection Act (DPDP) Act 2023 does not distinguish between personal data and sensitive personal data, particularly impacting the protection of health information from wearable devices. This broad classification approach lowers the protection standard and grants users less control over their health data, potentially allowing it to be shared or sold without their explicit consent. Additionally, the Act lacks specific provisions for special categories of data, a departure from previous regulations that offered enhanced protections for sensitive personal data, including health and biometric information. The absence of a higher consent threshold for sensitive data under the DPDP regime marks a significant change from prior legal frameworks that sought to safeguard such information more rigorously. The "legitimate purpose" clause in the DPDP Act 2023 raises concerns about ambiguity in informed consent for wearable data collection, potentially compromising user privacy and control. Pre-checked consent boxes in wearable technology compromise informed consent by obscuring details on data usage and pressuring users into all-or-nothing data collection decisions. This lack of transparency and undue pressure undermines the fundamental concept of meaningful user consent. This practice conflicts with the ideal of informed consent, where users should fully understand and willingly agree to how their sensitive data, like health information, is collected and used. clear, legally binding timelines for the deletion of personal data and stricter guidelines on the 'reasonable time' for data processing after consent withdrawal to enhance data protection have to adopted in the act. Despite recognising the flaws in consent-based approaches, efforts often mistakenly focus on enhancing the quantity rather than the clarity and quality of information provided to users.

Bundled service agreements and opaque data practices in wearables significantly limit user autonomy, potentially compromising personal privacy for functionality. The regulatory silence on anonymised data poses substantial re-identification risks, undermining user privacy and enabling discriminatory practices based on health data. This situation highlights the need for clear, transparent regulations that prioritise user consent and data protection to foster trust and innovation in wearable technology. The DPDP Act's failure to effectively address anonymised data, particularly in the context of health and location data from wearables, exposes users to

significant privacy risks, including re-identification and its consequences. Stricter regulations and increased user awareness are essential to mitigate these risks and protect individuals' privacy. there is a critical need for a security auditing mandate within the Digital Personal Data Protection Act for wearable technology organisations in India, advocating for regular audits by certified third-party vendors to enhance data protection. Such mandates ensure transparency, accountability, and the safeguarding of sensitive data against potential breaches. DPDP Act, does not Specify rights to data portability and to be forgotten, which are crucial for user privacy and control over personal information in the context of wearable technology. The DPDP Act of 2023 exposes wearable technology users to potential data security risks by not clearly distinguishing between "automated" and "digitised" data, thereby creating loopholes that may leave sensitive personal information unprotected. The establishment of the Data Protection Board of India, under the control of the central government, further stirs concerns about the effectiveness and independence of data regulation, hinting towards a surveillance-oriented approach. The DPDP Act of 2023 facilitates easier cross-border data transfers compared to the GDPR, posing potential security risks for wearable technology users due to less stringent restrictions except for countries on a "negative list." The legislation must adapt to adequately address these privacy concerns that arise, particularly with the proliferation of wearable devices.

CHAPTER 5

GLOBAL BEST PRACTICES

5.1 INTRODUCTION

As the preceding chapters have laid the groundwork on the intricacies of wearable technology data landscapes and meticulously examined the strengths and gaps inherent in the Digital Personal Data Protection Act 2023 (DPDPA 2023), it becomes imperative to extend our horizons beyond Indian borders.. This chapter explores how international data protection regulations, notably the European Union's General Data Protection Regulation (GDPR), the United States Health Insurance Portability and Accountability Act (HIPAA), and California's Consumer Privacy Act (CCPA), shape and influence the privacy landscape for wearable technologies worldwide. The chapter aims to dissect and analyse the key provisions of each regulation as they pertain to wearable devices, emphasizing their impact on data collection practices, user consent mechanisms, data security measures, and the rights of data subjects.

5.2 GENERAL DATA PROTECTION REGULATION (GDPR)

GDPR is one of the most comprehensive data protection regulations globally. It applies to any organisation processing personal data of EU residents, regardless of the organisation's location. GDPR imposes strict requirements on consent, transparency, and data minimisation. Wearable technology companies operating in the EU must adhere to GDPR's principles and ensure user data is collected and processed lawfully, fairly, and transparently.

- **Data Minimization**:
  In wearable technology, data minimisation involves collecting only the necessary personal data for the device's intended purpose. For example, a fitness tracker may only collect data on steps taken, heart rate, and sleep patterns rather than collecting additional unrelated data. GDPR Article 5(1)(c) states that personal data shall be adequate, relevant, and limited to what is necessary for the purposes for which it is processed. Article 25 emphasises data protection by design and by default, requiring controllers to implement appropriate technical and organisational measures, such as data minimisation, to ensure that only necessary data is processed.

- **Transparent Data Processing**:

Wearable technology manufacturers should provide clear information to users about how their data is collected, processed, and shared. This information can be conveyed through user manuals, privacy policies, and in-app notifications, ensuring users understand the implications of using the device. GDPR Article 12 mandates transparent communication with data subjects regarding processing their personal data, including providing concise, transparent, intelligible, and easily accessible information. Articles 13 and 14 outline the information that should be provided to data subjects at the time of data collection, including the identity of the controller, purposes of processing, recipients of data, and rights of the data subjects.

The GDPR grants the data subject extensive rights to get information about, change, or delete processed data and restrict its processing to specific purposes (Art. 12–23 GDPR). Data controllers and processors are obliged to inform the subjects fully, take precautions to protect personal data by design and default with technical and organisational measures, extensively record processing activities, and ensure data security (Art. 24–43 GDPR). For example, using encryption methods could lead to data not being considered personal data anymore, resulting in the GDPR not being applied to them in parts.[70] Article 21 of the GDPR also provides adequate protection for individuals, stipulating the individual's right to object to processing their data under certain circumstances, "including data processed for direct marketing purposes". Clarification about the further processing of health data is provided by the so-called "Informative Text" intended for National Contact Points in the "Cross-border Healthcare of Consumers, Health, Agriculture and Food Executive Agency" as set up by the EC. More specifically, processing personal health data, which is considered sensitive personal data, is prohibited – unless under specific circumstances, such as explicit consent of the data subject. At the same time, the latter has the right to object. These rights imply that the individual needs the possibility to know who the controller or a third party is. As such, the controllers should comply with the GDPR. Many

[70]Gerald Spindler and Philipp Schmechel, "Personal Data and Encryption in the European General Data Protection Regulation" 2 (2016): 163.

companies, such as Garmin or BV Wearable Stories, include provisions on the right to object in their privacy statements.[71]

- **Secure Data Storage and Transmission**:

Wearable IoT devices store sensitive personal data, such as health and fitness information, making secure data storage and transmission crucial. Encryption and authentication mechanisms should be implemented to protect data at rest and in transit, minimising the risk of unauthorised access or data breaches. GDPR Article 32 requires controllers and processors to implement appropriate technical and organisational measures to ensure security appropriate to the risk, including the pseudonymisation and encryption of personal data. This aligns with the confidentiality, integrity, availability, and resilience principles outlined in Article 5(1)(f).

One of the more controversial rules of GDPR states that controllers and processors must ensure that data are only transferred to third countries or international organisations if these states or organisations comply with the GDPR or provide an equally high standard of data protection (Art. 44–50 GDPR). In its judgement, "Schrems II"[72], the European Court of Justice determined that the United States does not fulfil the high standards of GDPR; this ruling affects the use of, for example, U.S.-based cloud data storage services by requiring extensive contract clauses regarding the processing of personal data [73]. Without such clauses, even the simple storage of healthcare data of European users (for example, smart wearables for cardiac monitoring) on U.S.-based clouds (such as Azure, AWS, or the like) is prohibited. This decision will apply until the EU Commission passes a new "adequacy decision" regarding data transfers to the United States.[74]

[71] Garmin, "Privacy Policy" (Garmin, April 2022) accessed 23 May 2022. Also see: WS Wearable Stories, 'Privacy Statement' (WS, February 2021) accessed 23 May 2022

[72] Judgement of the Court of Justice of the European Union, 16 July 2020, Case C-311/18, ECLI:EU:C:2020:559, Facebook Ireland and Schrems.

[73] Christopher, K. Schrems II Re-Examined.

[74] Jan Benedikt Brönneke et al., "Regulatory, Legal, and Market Aspects of Smart Wearables for Cardiac Monitoring," Sensors 21, no. 14 (July 20, 2021): 4937, https://doi.org/10.3390/s21144937.

- **Privacy by Design and Default**:
  Wearable technology should incorporate privacy-enhancing features by design, such as allowing users to control the sharing of their data and enabling pseudonymisation of personal information. Default settings should prioritise user privacy, ensuring that data collection and sharing are minimised unless explicitly configured otherwise by the user. Article 25 mandates that data protection principles be integrated into processing systems, services design, and default settings. This encompasses implementing measures such as data minimisation, pseudonymisation, and user-centric privacy settings from the outset, aligning with the GDPR's emphasis on proactive privacy protection.

- **User Consent and Control**:
  Users should provide explicit consent before wearable IoT devices collect and process their data. This consent should be granular, allowing users to specify the types of data they are comfortable sharing and allowing them to revoke consent at any time. GDPR Articles 6 and 7 outline the conditions for the lawful processing of personal data, emphasising the requirement for freely given, specific, informed, and unambiguous consent from the data subject. Article 9 addresses the processing of special categories of personal data, including health data collected by wearable IoT devices, requiring explicit consent from data subjects.

- **Data Protection Impact Assessments (DPIAs)**:
  Wearable technology manufacturers should conduct DPIAs to assess the privacy risks associated with their devices. This includes evaluating the potential impact on user privacy and implementing measures to mitigate identified risks, such as anonymising data to protect user identities.GDPR Article 35 requires controllers to conduct DPIAs for processing activities that are likely to result in high risks to the rights and freedoms of data subjects.DPIAs help assess and mitigate privacy risks associated with wearable IoT devices, ensuring compliance with the GDPR's accountability principle outlined in Article 5(2).

- **Data Breach Response Plan**:

  Wearable technology companies should have a comprehensive data breach response plan to detect, investigate, and mitigate data breaches. This includes promptly notifying supervisory authorities and affected individuals of GDPR requirements to minimise the breach's impact on user privacy. GDPR Article 33 mandates the notification of personal data breaches to the supervisory authority without undue delay unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. Article 34 requires controllers to communicate personal data breaches to affected subjects without undue delay when the breach is likely to result in a high risk to their rights and freedoms.

- **Data Subject Rights**:

  Wearable technology users have rights under the GDPR to access, rectify, and delete the data stored by the device. Manufacturers should provide mechanisms for users to exercise these rights, such as through dedicated user portals or support channels. GDPR Articles 15-22 grant data subjects various rights, including the right to access, rectify, erase, and restrict the processing of their personal data. Controllers must facilitate the exercise of these rights by providing mechanisms for data subjects to submit requests and receive timely responses, as outlined in Article 12. Article 15 of the GDPR, whereby individuals have the right to request a copy of any of their personal data, including other relevant information being processed by controllers. This right includes data concerning their health, according to Article 4 (15). Moreover, this right was clarified under Recital 63, according to which "a data subject should have the right to access his/her personal data that have been collected, including data on his/her health".[75]

- **Vendor Management**:

  GDPR Article 28 requires controllers to enter into written contracts with processors that include specific provisions regarding data processing, security measures, and compliance with GDPR requirements. Controllers are responsible for ensuring that third-party vendors and service providers adhere to GDPR obligations, including implementing appropriate technical and organisational measures to protect personal data. Wearable technology manufacturers must ensure that third-party vendors and

[75] Recital 63, Right of Access, General Data Protection Regulation May 2022

service providers in the device ecosystem comply with GDPR requirements. This includes entering into contracts that specify data processing obligations and conducting regular assessments to verify compliance.

- **Regular Compliance Audits**:

  While not explicitly mentioned in specific articles, regular compliance audits are essential for ensuring ongoing compliance with the GDPR's requirements. Article 24 requires controllers to demonstrate compliance with the GDPR's principles and obligations, which necessitates regular assessments of data processing activities and associated measures. Wearable technology manufacturers should conduct regular compliance audits to evaluate their adherence to GDPR requirements. This involves reviewing data processing activities, security measures, and privacy practices to identify any areas for improvement and ensure ongoing compliance.

By implementing these GDPR best practices in developing and operating wearable IoT devices, manufacturers can enhance user privacy protections and mitigate regulatory risks associated with data processing. Article 110 of the European MDR, for example, explicitly requires the application of the GDPR and declares compliance with the GDPR's rules mandatory for receiving a CE mark. Compliance with privacy and data security regulations becomes even more critical if the wearable is sought to be used within a (public) healthcare system and reimbursed by health insurers. Because these institutions (as well as health care providers themselves) fall under prevailing domestic or regional data protection and security regulations, the use of non-compliant devices is often prohibited and, at a minimum, would be expected to come with the cost of losing trust among patients and other parties in the health care system. Although potentially challenging, compliance with the target market's respective privacy and data security rules is essential for successful market access to intelligent wearables for cardiac monitoring.[76]

By aligning with these specific articles and principles of the GDPR, manufacturers and developers can effectively implement GDPR in wearable IoT devices, safeguarding user privacy and mitigating regulatory risks.

[76] Jan Benedikt Brönneke et al., "Regulatory, Legal, and Market Aspects of Smart Wearables for Cardiac Monitoring," Sensors 21, no. 14 (July 20, 2021): 4937, https://doi.org/10.3390/s21144937.

5.3 HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA)

Adherence to HIPAA regulations is essential when wearable devices involve protected health information (PHI). Understanding how HIPAA intersects with wearable health technology is pivotal. Regarding personal health information, the primary law that protects health information is the Health Information Portability and Accountability Act, or simply HIPAA. In the United States, the primary federal regulation for personal health data is the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule. This rule was the first to establish a set of national standards for safeguarding individually identifiable health information, known as personal health information (PHI)[77]. HIPAA primarily addresses practices related to individual consent, retention, security, and the transfer of PHI. PHI is legally defined as "any information about health status, provision of health care, or payment for health care created or collected by a covered entity (primarily health care providers and health plans) that can be linked to a specific individual." [78]. HIPAA and its regulations require subjects (healthcare providers, health plans, etc.) and their partners (associates) to comply with multiple data privacy and security requirements. In essence, HIPAA prohibits the subjects stated above from sharing a patient's personal and identifiable health information with third parties without the patient's consent. [79]. However, the Privacy Rule includes many exceptions to this general rule on sharing a patient's information; law enforcement is an exception. In cases where there is a warrant or subpoena, healthcare providers, for example, may disclose their patients' health data. While these exceptions might limit a person's privacy rights, HIPAA offers protection regarding a person's health records. The HIPAA "Security Rule" of 1996 mandates that entities accessing PHI must "ensure the confidentiality, integrity, and availability" of this health information. Additionally, these entities must notify affected individuals "without unreasonable delay" in the event of a personal data breach.

A primary limitation of HIPAA is that it does not provide those protections when patients use digital tools to record, save, disclose, monitor, or manage their health information. In fact, most

[77] Rajakariar, K.; Buntine, P.; Ghaly, A.; Zhu, Z.C.; Abeygunawardana, V.; Visakhamoorthy, S.; Owen, P.J.; Tham, S.; Hackett, L.; Roberts, L.; et al. Accuracy of Smartwatch Pulse Oximetry Measurements in Hospitalized Patients with Coronavirus Disease 2019. *Mayo Clin. Proc. Digit. Health* **2024**, *2*, 152–158.
[78] Ibid
[79] "Understanding HIPAA for Law Firms," Thomson Reuters Legal, n.d., https://legal.thomsonreuters.com/en/insights/articles/understanding-hipaa-for-law-firms.

digital health apps are not considered medical devices and thus do not require FDA approval[80]. The data being shared with and collected by these apps are managed by the software vendors and inaccessible by healthcare providers, therefore falling outside the HIPAA regulations[81]. More specifically, when a doctor forwards a patient's health data to either the patient or a third-party app designated by the patient, and subsequently, the patient or the app misuses or experiences a data breach, the doctor's health system is not held accountable under HIPAA. Instead, the responsibility falls upon the patient or the third party.

Here are some key considerations:

1. **HIPAA Compliance Requirement for Patient Data**:

   HIPAA compliance is crucial when a company's wearable device requires patients to provide Protected Health Information (PHI). Patients may voluntarily share personal information, such as age and weight, for accurate readings on a wearable blood pressure monitor. HIPAA comes into effect when healthcare providers integrate this sensitive patient data with electronic health records (EHRs) and other systems used by healthcare facilities and insurance providers, mandating compliance with the Privacy Rule for safeguarding patient information.

   Under HIPAA, covered entities (such as healthcare providers) and their business associates must comply with the Privacy Rule when handling protected health information (PHI). This includes implementing measures to ensure the confidentiality, integrity, and availability of PHI, providing individuals with access to their health information, and notifying them in the event of a breach.[82] Section 1173 of HIPAA Title II: Administrative Simplification, Subtitle F: Miscellaneous Provisions outlines the standards for information transactions and data elements, which includes the requirements for electronic health information exchange.

[80] I. Glenn Cohen, "Informed Consent and Medical Artificial Intelligence: What to Tell the Patient?," The Georgetown Law Journal, vol. 108, 2020.
[81]Sean Hooley and Latanya Sweeney, "Survey of Publicly Available State Health Databases," Social Science Research Network, January 1, 2013, https://doi.org/10.2139/ssrn.2277688.
[82] Asma Sifaoui and Matthew S. Eastin, "'Whispers from the Wrist': Wearable Health Monitoring Devices and Privacy Regulations in the U.S.: The Loopholes, the Challenges, and the Opportunities," Cryptography 8, no. 2 (June 19, 2024): 26, https://doi.org/10.3390/cryptography8020026.

2. **Informing Patients about Data Collection Policies:**

Protecting patient data involves informing them of data collection policies. HIPAA mandates providers to communicate how data is collected, stored, and used. Therefore, users must understand privacy and security practices if a healthcare facility collects data from wearable devices, such as sleep patterns from an Apple Watch app.HIPAA requires covered entities to notify individuals of their privacy practices, including how their Protected Health Information (PHI) will be collected, used, and disclosed. This notice must be provided clearly and concisely, allowing patients to make informed decisions about their health data. Section:164,520 of HIPAA Title II: Administrative Simplification, Subtitle F: Miscellaneous outlines Notice of privacy practices for protected health information

3. **HIPAA Compliance for Providing Wearables**:

In the pursuit of competitiveness, healthcare providers and insurance companies may incentivise data sharing through wearable devices. This shift towards using wearables for healthcare data necessitates more HIPAA-compliant devices. Providers offering wearables to patients or engaging third-party developers must ensure HIPAA compliance, especially under the Security Rule. The Security Rule under HIPAA mandates covered entities to implement safeguards to protect electronic PHI (ePHI).Section 164.312 of HIPAA Title II: Administrative Simplification, Subtitle F: Miscellaneous Provisions outlines Technical safeguards.

4. **Separate Data Collection Setup**:

Studies using wearable devices, such as electrocardiogram (ECG) patches for diagnosing atrial fibrillation (AFib), underscore the need for secure data transmission. Since wearables handle Protected Health Information (PHI), ensuring compliance with HIPAA is crucial. This requires implementing secure data encryption before transmission to healthcare systems. Alternatively, a separate data collection setup may be necessary to summarise and encrypt patient data before transfer. This approach can help ensure that the PHI collected by the wearable device is adequately secured and protected before it is integrated into the healthcare provider's systems.

Covered entities must ensure that any electronic Protected Health Information (ePHI) transmission is secure, such as through encryption, to comply with the HIPAA Security Rule. This includes implementing technical safeguards to protect the confidentiality, integrity, and availability of ePHI during transmission and storage. The HIPAA Security Rule (45 CFR §

164.312) outlines the specific technical safeguards that covered entities must implement, including:

- Access controls: Implementing measures to limit access to ePHI to only authorised individuals or entities.
- Audit controls: Implementing hardware, software, and/or procedural mechanisms to record and examine activity in information systems that contain or use ePHI.
- Integrity controls: Implementing policies and procedures to protect ePHI from improper alteration or destruction.
- Transmission security: Implementing technical security measures to guard against unauthorised access to ePHI that is being transmitted over an electronic communications network.

By implementing these technical safeguards, healthcare providers and wearable device manufacturers can ensure that the PHI collected by smart wearables is adequately secured and protected in compliance with HIPAA regulations.

5. **Minimum Necessary Requirement**:

HIPAA's Privacy Rule limits PHI requests to only what's necessary for the wearable device's intended purpose. For instance, if a device tracks exercise progress, the information requested should be limited to relevant data. Unnecessary information, like user location, should not be solicited unless essential for the device's function. The Privacy Rule requires covered entities to limit the use or disclosure of PHI to the minimum necessary to accomplish the intended purpose. Section 164.502 HIPAA Title II: Administrative Simplification, Subtitle F outlines Miscellaneous Provisions - Uses and disclosures of protected health information.

HIPAA comprises the Privacy Rule, which sets national standards for protecting individually identifiable health information held by covered entities like health plans, clearinghouses, and health care providers. It distinguishes permissions for using protected health information (PHI), often making individual consent unnecessary within covered entities. Complementing this, the Security Rule establishes standards for securing electronic PHI (ePHI). Manufacturers of wearable technology that contract with HIPAA-covered entities must ensure compliance with these rules, which include implementing safeguards to protect PHI. Unlike the European GDPR, HIPAA's scope is narrower. It applies specifically to health-related entities,

underscoring the importance of manufacturers understanding and adhering to these regulations when designing and deploying health-related wearable devices.

5.4THE CALIFORNIA CONSUMER PRIVACY ACT (CCPA)

The California Consumer Privacy Act (CCPA) is a comprehensive data privacy law that enhances consumer protections for residents of California. This act has significant implications for companies developing or selling wearable technology within the state, dictating the manner in which personal information is collected, handled, and protected. Understanding the CCPA is essential for these companies to not only comply with legal requirements but also to foster trust and transparency with their users, ensuring that personal data is safeguarded against unauthorized access and misuse. Regarding wearable technology, such as fitness trackers, smartwatches, or health monitoring devices, the CCPA has implications primarily in how personal data collected by these devices is handled and protected.

- Personal Information: The CCPA defines "personal information" broadly, including identifiers like name, email address, and also more unique identifiers such as device IDs, IP addresses, and geolocation data under CCPA Section 1798.140(o), Data collected by wearable technology often falls within this definition, especially if it can be linked back to an individual.

- Consumer Rights: Under the CCPA, California consumers have several rights regarding their personal information, including the right to know what personal information is being collected, used, shared, or sold by companies. Wearable technology companies must disclose these practices to consumers. CCPA Section 1798.100 grants California consumers rights regarding their personal information, including the right to know what personal information is being collected (1798.110), the right to request deletion of personal information (1798.105), and the right to opt out of the sale of personal information (1798.120).

- Notice at Collection: Companies that collect personal information through wearable technology must notify consumers at or before the point of collection. This notice should inform consumers about the categories of personal information being collected and the purposes for which it will be used. CCPA Section 1798.100(b) requires businesses that

collect personal information through wearable technology to inform consumers at or before the point of collection about the categories of personal information to be collected and the purposes for which the information will be used.

- Opt-Out Rights: Consumers have the right to opt out of selling their personal information to third parties. This is particularly relevant if wearable technology companies share personal data with advertisers or other entities.

- Data Security: The CCPA requires businesses to implement reasonable security measures to protect consumers' personal information from unauthorised access, destruction, use, modification, or disclosure. Companies must implement reasonable security measures to protect consumers' personal information under CCPA Section 1798.150.

- Children's Privacy: If wearable technology is designed for children under 16, additional requirements apply, such as obtaining opt-in consent from a parent or guardian before selling the child's personal information. CCPA Section 1798.120(c) requires businesses to obtain opt-in consent from a parent or guardian before selling the personal information of children under 16.

- Non-Discrimination: Businesses cannot discriminate against consumers who exercise their CCPA rights, such as by denying them goods or services, charging them different prices, or providing them with a different level or quality of service. CCPA Section 1798.125 prohibits businesses from discriminating against consumers who exercise their CCPA rights, such as by denying goods or services, charging different prices, or providing a different level or quality of goods or services

For companies developing or selling wearable technology in California, compliance with the CCPA is crucial to avoid potential fines and legal issues. It's essential to regularly review and update privacy policies, implement data protection measures, and ensure transparency in data practices to align with CCPA requirements.

Compared to the Digital Personal Data Protection Act 2023 (DPDPA 2023) in India, several jurisdictions have developed more comprehensive or specific frameworks that offer enhanced privacy protections. For instance, the European Union's General Data Protection Regulation (GDPR) sets a worldwide benchmark for data privacy laws, offering individuals greater control over their data. The GDPR's principles of data minimisation, consent, and right to erasure are particularly relevant for wearable technology, emphasising user consent and limiting data collection to the minimum necessary. This contrasts with the DPDPA 2023, which, while robust, may lack the same level of explicit controls over data minimisation and user consent in the context of wearable devices. The patchwork of federal and state-level regulations in the United States presents a different picture. While no single comprehensive federal law like the GDPR or DPDPA 2023, specific states such as California, with its California Consumer Privacy Act (CCPA), offer protections that mirror and, in some aspects, surpass those under the DPDPA 2023. The CCPA's provisions for transparency and the right to opt out of the sale of personal information are commendable; however, its application to wearable technologies is not as explicit as it could be, leaving room for interpretation. The Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada also provides a valuable comparison, particularly its emphasis on the principles of accountability and consent. While similar to the scope of DPDPA 2023, PIPEDA's application to wearable technology showcases the importance of accountability in processing personal data, setting a precedent that could further strengthen the DPDPA 2023's effectiveness.

5.5 CONCLUSION

Compared to the Digital Personal Data Protection Act 2023 (DPDPA 2023) in India, several jurisdictions have developed more comprehensive or specific frameworks that offer enhanced privacy protections. For instance, the European Union's General Data Protection Regulation (GDPR) sets a worldwide benchmark for data privacy laws, offering individuals greater control over their data. GDPR particularly impacts wearable technology companies, requiring them to collect only necessary data and ensure users are fully informed about their data's usage and rights, including access, correction, and deletion. Additionally, the GDPR emphasizes the importance of secure data handling, necessitating the implementation of technical and organizational measures like encryption for data protection, and carefully regulating data transfer to non-EU countries to maintain high privacy standards. To ensure compliance with

GDPR and mitigate regulatory risks, wearable IoT device manufacturers are regulated as to implement specific data protection and security measures, including entering into contracts with third-party vendors, conducting regular compliance audits, and aligning with GDPR and local data protection regulations, especially when seeking market access in healthcare. HIPAA compliance is critical for companies integrating patient data from wearable devices with health records, requiring safeguards for Protected Health Information (PHI) and clear communication to patients about data collection policies. Healthcare providers offering wearables must ensure these devices are HIPAA compliant, particularly under the Privacy and Security Rules, to protect electronic PHI and maintain patient trust. Studies using wearable devices for health monitoring, like ECG patches for AFib, highlight the importance of secure data transmission and compliance with HIPAA, necessitating encryption of Protected Health Information (PHI) before it reaches healthcare systems. HIPAA regulations mandate technical safeguards for electronic PHI (ePHI), including access, audit, and integrity controls, as well as transmission security, to protect data confidentiality, integrity, and availability, with the Privacy Rule further restricting PHI usage to the minimum necessary for the device's intended purpose.

The California Consumer Privacy Act (CCPA) represents a comprehensive data privacy law that mandates strict handling and protection of personal information by companies operating with wearable technology in California, addressing everything from collection to consumer rights. It broadly defines personal information, covering identifiers from names to geolocation data, and grants California consumers extensive rights including the ability to know about and opt out of the sale of their data. Companies are required to notify consumers about the collection of personal data at or before the point it is collected, ensuring transparency about the types of data collected and its uses. Additionally, the CCPA emphasizes the importance of data security and children's privacy and prohibits discrimination against consumers who exercise their rights under the act. The DPDPA 2023 represents a significant step forward for India. Still, integrating lessons from regulations around the world can strengthen digital personal data protection and combat data privacy issues in evolving wearable technology.

CHAPTER 6

CONCLUSION AND SUGGESTIONS

6.1 OVERVIEW

Wearable technology devices are broad in type— fitness trackers, smartwatches, health monitors, and smart apparel — each serving different needs but unified in their capacity to collect intimate details about the user. From heart rate measurements, physical activity levels, and sleep patterns, to more complex data like GPS locations and even psychological states inferred from biometric data, the scope is vast and deeply integrated into personal lives. while these devices offer unprecedented insights into individual health and behavior, they also open floodgates to privacy breaches if the data is mishandled or inadequately protected.

Wearable technologies encompass a wide variety of devices that collect an exhaustive range of highly sensitive data. There is inherent privacy and security vulnerabilities associated with the collection of sensitive personal data by wearables. There is pressing need for stringent data protection mechanisms to safeguard this data against unauthorized access and exploitation. Enhanced consumer awareness regarding the extent of data collection by wearables and the potential privacy implications are also essential. It suggests that informed user regulations are essential for better privacy protections and more ethical data handling practices by manufacturers. Such frameworks should not only entail regulations governing the collection, use, and sharing of data but also foster practices that prioritise user consent, data minimization, and transparency.

The Digital Personal Data Protection Act, 2023 (DPDPA) is a landmark legislation enacted by the Parliament of India to safeguard the digital personal data of citizens.It introduces key definitions such as Data Fiduciary, Data Principal, Data Processor, and outlines terms relating to data handling like gain, loss, and harm, aiding a comprehensive grasp of its scope and implications. A major provision is the prevention of unauthorized data collection by Data Fiduciaries, permitting data processing, storage, or transfer solely for the collected purpose. The Act's scope is primarily within India, focusing on the handling of personal data in digital form. It applies to data gathered online or offline but later digitised, and extends to processing outside India if it involves offering goods or services to individuals within India. Exceptions are made for personal or household use, legally mandated disclosures, or data used for research, archiving, or statistical purposes under specific conditions.

Personal Data is defined broadly within the Act to include any information relating to an identifiable individual, with a focus on data in digital form. The Act outlines a comprehensive approach to data processing, including collection, storage, use, and destruction, ensuring personal data pertains to identified or identifiable individuals. This sets the framework for how businesses and government entities must handle personal data. The obligations of Data Fiduciaries are expanded, especially for those categorised as Significant Data Fiduciaries, who are subject to additional requirements like periodic audits and Data Protection Impact Assessments. These fiduciaries must adhere to the Act's stipulations, including setting up grievance redressal mechanisms and maintaining the accuracy and completeness of personal information. Data must be erased if user consent is withdrawn or the data's purpose is deemed irrelevant, with stipulations made for legal mandates to retain data. Lastly, the Act introduces a detailed consent framework, emphasising that consent must be free, specific, informed, unconditional, and unmistakable, with a limit to the validity of consent to the necessary data for the specified purpose. Data Principals have the right to withdraw their consent, with provisions for the use of Consent Managers to facilitate this process. This ensures a systematic approach for users to control their personal data.

However there is certain complexity of applying general digital data protection laws to the unique challenges presented by wearable technology.The critical analysis identifies gaps and loopholes that could compromise data privacy in the context of rapidly evolving wearable technologies. Issues such as the adequacy of consent mechanisms, the applicability of the act to international entities handling data of Indian users, and the enforcement mechanisms to protect the rights established by the law are discussed.

The DPDP Act 2023 is criticised for its broad classification of data, which does not explicitly categorise health data collected by wearables as "sensitive." This results in a lower protection standard for such data than those offered under frameworks like the GDPR. Due to the lack of differentiation between "personal data" and "sensitive personal data," users may have limited control over their health data. This opens up potential scenarios where users are unaware of how their health data is shared or sold to third parties, undermining privacy protections. The analysis underscores significant areas where the DPDP Act 2023 falls short, especially concerning the unique challenges of wearable technology data. There is a need for specific provisions that better protect sensitive health information and ensure users have greater control and awareness of how their data is used. It is identified that the conventional mechanisms for obtaining user consent, as currently outlined in the legislation, may not be adequate for

wearables' continuous and pervasive data collection. The need for more dynamic and contextual consent processes is highlighted. It was found that the principle of data minimisation—a core tenet of the Act—is particularly challenging to implement in the context of wearables. These devices, by design, collect vast amounts of data, often more than what is immediately necessary, complicating compliance with this principle. The findings suggest that the rights granted to users under the Act related to accessing, correcting, and deleting their data need reinforcement. This is particularly important for wearable device users who may have continuous and varied data collected about them.

It is important to look beyond the Indian context to understand how the rest of the world is managing the privacy challenges posed by wearable devices. The European Union's General Data Protection Regulation (GDPR), the United States' Health Insurance Portability and Accountability Act (HIPAA), and California's Consumer Privacy Act (CCPA) are identified as critical regulatory frameworks that influence global data protection standards for wearable technologies. The GDPR is highlighted for its comprehensive approach to personal data protection, applying broad requirements for consent, transparency, and data minimisation on any entity processing the data of EU residents. This move necessitates that companies operating wearable technologies within the EU ensure that data collection and processing are lawful, fair, and transparent, adhering strictly to the GDPR's mandates. For wearable devices collecting PHI, HIPAA compliance is paramount, necessitating strict adherence to its privacy rules when integrating data into electronic health records (EHRs). Moreover, healthcare providers must clearly inform patients about how their data is collected, used, and protected, ensuring transparency and maintaining trust. CCPA grants consumers significant rights, including being informed about data collection practices, requesting to delete their personal information and opt out of their data being sold. Notably, businesses must provide clear notice to consumers at the point of data collection, detailing what information is being collected and for what purpose. Moreover, the CCPA highlights the importance of securing consumer data against unauthorised access and outlines specific provisions for protecting children's privacy, necessitating parental consent for data sales involving those under 16. It also prohibits any form of discrimination against consumers who exercise their rights under the act.the GDPR mandates that personal data must be relevant and limited to what is needed, underlining the importance of designing devices that inherently protect user data by minimising data collection and processing. The narrative further explores the need for clear communication with users about data collection

and processing activities. This aligns with GDPR's requirement for transparency, ensuring that users are well-informed about managing their data.

The extensive rights granted to data subjects under these legal frameworks, including the right to access, modify, and delete personal data, highlight the significant responsibilities placed on data controllers and processors to maintain the integrity and security of personal data. Furthermore, the discussion underscores the potential benefits of adopting these stringent data protection measures, suggesting that they could enhance user trust and compliance and pave the way for global standardisation in the fast-evolving domain of wearable technology.

By addressing these observations, there is potential to significantly strengthen the DPDP Act 2023, making it more effective in protecting the privacy of individuals in the context of wearable technology.

6.2 KEY FINDINGS

This study embarks on an insightful journey to evaluate the efficacy of the Digital Personal Data Protection Act 2023, with a specific lens on wearable technology. Through a comprehensive analysis of legal documents, technological reports, and literature, the following key findings have been identified:

- Proliferation and Variability of Wearable Technologies: The market has seen rapid proliferation and evolution of wearable technologies, transitioning from simple external sensors in sportswear to sophisticated embedded and garment-integrated sensors. This evolution has introduced complex data privacy and protection challenges.
- Increased Privacy Risks: Consistent with concerns raised in the literature, wearable technologies enhance the potential for surveillance and unauthorised data use. These devices generate enormous amounts of personal data, making users vulnerable to privacy invasions if data is not adequately protected.
- Gaps in Legislation: The Digital Personal Data Protection Act 2023 represents a significant step forward in the legal protection of personal data in India. However, findings suggest gaps, particularly concerning the unique challenges the data collected through wearable technologies poses. There are areas where the Act could be more specific or prescriptive in addressing the nuanced risks associated with wearable devices.

- Specificity to Wearable Technology: The Act, while robust in several aspects, seems to lack specificity when addressing the unique data collection, processing, and storage mechanisms inherent to wearable technologies. Since these devices continuously collect personal and sensitive data such as health metrics, geographical locations, and even behavioural patterns, there is a need for clauses that specifically address the consent mechanism, data anonymisation, and encryption standards tailored for wearables.
- Continuous Data Collection: Wearable technologies are characterised by their ability to collect data continuously and in real-time. This constant data collection poses unique privacy risks not fully contemplated by the Act. For instance, there is a gap in the regulation regarding continuous consent – where users may need to be prompted for their consent periodically, given the changing nature of the data collected over time.
- Data Minimization Principle: While the Act emphasises the importance of data protection and privacy, it could further elaborate on the principle of data minimisation, specifically for wearables. This principle advocates for collecting only the data necessary for a specified purpose. Given the vast amount of unnecessary data wearable devices could collect, clear guidelines on data minimisation for wearable manufacturers and developers are essential.
- Data Sharing with Third Parties: Wearable devices often integrate with third-party services for enhanced functionality, raising concerns about data sharing and user consent. The Act could more explicitly address the conditions under which data collected by wearables can be shared with third parties, ensuring that users have clear information and control over how their data is used beyond the primary service providers.
- Security Standards for Wearable Data: Given the sensitive nature of data collected by wearable technologies, the Act would benefit from including specific security standards or requirements for the encryption and protection of this data. This would help ensure that data, whether at rest or in transit, is adequately protected against unauthorised access or breaches.
- Future-Proofing Legislation: Wearable technology rapidly evolves, bringing about new capabilities and privacy concerns. The legislation gaps reveal a need for the Act to be agile and easily amendable to adapt to future advancements in wearable

tech. This could involve establishing a framework or body dedicated to ongoing assessment and recommendation of updates to the law as technology advances.

Addressing these gaps would strengthen the efficacy of the Digital Personal Data Protection Act 2023 in safeguarding privacy rights and ensure it remains relevant and robust in the face of rapidly evolving technological landscapes.

- Comparison with International Standards: When compared to data privacy regulations and standards in other countries and as per international guidelines, the Act is robust but still has room for improvement. Specifically, regarding the constant evolution of wearable technology, ongoing updates and revisions to the Act might be necessary to keep pace with technological advancements and emerging privacy risks.

- International Benchmarking: Countries around the globe have adopted various approaches to data privacy and protection, each with unique strengths. For instance, the General Data Protection Regulation (GDPR) in the European Union is often hailed for its stringent data protection standards, offering a potential benchmark. GDPR provides explicit rights to individuals regarding their data, such as the right to be forgotten, and imposes heavy fines for non-compliance, which might be more deterrent than those under the Indian Act. Similar comprehensive data protection acts, like the California Consumer Privacy Act (CCPA) in the United States, emphasise consumer rights over personal information, introducing concepts like data portability and transparency in data collection practices. The Health Insurance Portability and Accountability Act (HIPAA) in the United States further illuminates areas for enhancement, especially concerning wearable technology. HIPAA, primarily focused on protecting patient health information and medical records, offers insights into stringent privacy and security measures despite its non-direct applicability to all wearable technologies.
- Comparative Efficiency: When compared, the Digital Personal Data Protection Act 2023 incorporates several robust provisions. Still, it falls short in certain aspects, particularly concerning the granularity of user consent, data minimisation, and transparency requirements in international standards like GDPR. Moreover, the efficiency of enforcement mechanisms and the extent of penalties for breaches under the Indian Act do not parallel the more stringent counterparts in these international regulations. The absence of a dedicated independent supervisory authority to oversee

compliance and grievances related to wearable technologies under the Indian framework is another point of divergence.

- Adaptation to Wearable Technology: Specific to wearable technology, international guidelines often propose more detailed frameworks addressing the continuous data collection, processing, and cross-border data transfer challenges peculiar to these devices. The lack of detailed provisions in the Indian Act regarding the same underscores an area ripe for enhancement. For example, the GDPR requires impact assessments for high-risk data processing activities, which could include certain functions of wearable technologies, thereby ensuring that any potential risks to individual privacy are evaluated and mitigated before products are introduced to the market.

In conclusion, while the Digital Personal Data Protection Act 2023 signifies a critical legislative effort to protect personal data, wearable technology's unique and evolving landscape demands continuous assessment and adaptation of these legal frameworks. Adopting a dynamic, multi-stakeholder approach could significantly enhance the effectiveness of data protection measures for wearable technologies in India.

6.3 SUGGESTIONS

Here are some suggestions based on the findings from the dissertation;

- **Strengthening Consent Mechanisms**:

  The Act emphasises informed and unambiguous consent. However, there is room for improvement in ensuring that consent is significant. Data fiduciaries should provide clear, concise explanations of data processing purposes. Implement user-friendly interfaces for consent management, allowing individuals to understand and control their data efficiently.

- **Enhancing Data Security and Breach Reporting**:

  While the Act mandates reporting data breaches, there is a need for more robust security measures and regular security audits and vulnerability assessments should be conducted. The NIST (National Institute of Standards and Technology) has published guidelines to help organisations detect, respond to, and recover from data breaches. These guidelines are particularly relevant for safeguarding data confidentiality.

- Detection: Implement intrusion detection systems (IDS), security information and event management (SIEM) tools, and network monitoring solutions. These technologies help identify suspicious activities or anomalies. Regularly analyse logs from various systems (e.g., servers, firewalls, applications) to spot signs of unauthorised access, malware, or unusual behaviour. Stay informed about emerging threats and attack patterns. Leverage threat intelligence feeds and collaborate with industry peers.
- Containment: When a breach is detected, isolate compromised systems to prevent further attack spread. This may involve network segmentation or disabling affected accounts. Address any known vulnerabilities promptly. Apply security patches to affected software or systems. Reset passwords for compromised accounts and revoke access tokens.
- Recovery: Regularly back up critical data and systems. In case of a breach, restore clean backups to minimise downtime. Have a well-defined incident response plan that outlines roles, responsibilities, and communication channels during a breach. Conduct a thorough investigation to understand the scope of the breach, identify the attack vector, and assess the impact. Comply with legal requirements (such as breach notification laws) and report the incident to relevant authorities.[83]

These guidelines are part of NIST's SP 1800-29: Data Confidentiality series, which focuses on protecting assets against data breaches. Incorporating these practices can significantly enhance the ability to handle data breaches effectively.

- **Balancing Privacy and Innovation:**

The Act aims to protect privacy but should not hinder technological advancements. Encourage research and development of privacy-preserving technologies—Foster collaboration between industry, academia, and regulators to strike the right balance.

- **Clarifying Definitions and Scope:**

Some terms, such as "persons with disabilities," need more explicit definitions. Provide specific criteria for identifying persons with disabilities. Clarify the scope of the Act regarding cross-border data transfers.

[83] https://csrc.nist.gov/pubs/sp/1800/29/final

- **Empowering Data Principals:**

  Data principals should have more control over their data.Recommendations.Strengthen data subject rights, including the right to data portability. Promote awareness campaigns to educate individuals about their rights—the concept of "data trusts" as a mechanism for giving individuals more control over their data. Data trusts act as fiduciaries, managing data on behalf of beneficiaries.[84]

- **Monitoring and Enforcement**:

  The Data Protection Board (DPB) plays a crucial role in enforcing the Act. Ensure the DPB has adequate resources and expertise. Establish transparent processes for handling complaints and imposing penalties. International data protection agreements recognise the fundamental right to data protection. To effectively enforce this right, legislation must establish an independent supervisory authority. Such an authority requires a clear statutory mandate, powers, and independence. It plays a crucial role in overseeing and enforcing data protection frameworks. Most countries (90%) with data protection laws opt for an independent supervisory authority. Examples include the EU's General Data Protection Regulation (GDPR) and the Council of Europe's Convention 108. Some countries combine functions, having a single institution regulating access to information and data protection. However, this should not compromise the authority's independence. For instance, Germany has state-level regulators and a Federal Data Protection Commissioner overseeing federal bodies. Multiple independent supervisory authorities can also exist, each with a specific jurisdiction.

  Laws should define the authority's composition, required expertise, and appointment process. Sufficient resources (financial, technical, and human) are essential. The authority must remain free from external influence and incompatible actions. Independence ensures effective enforcement. The authority monitors compliance with data protection laws. Regular reviews of entities subject to the law are crucial.[85] Independent supervisory

[84] Bennett Moses, L., & Chan, J. (2019). *Data Trusts: Creating a Fair and Just Digital Economy*. The Ada Lovelace Institute.

[85]Bamberger, K. A., & Mulligan, D. K. (2013). *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe*. MIT Press.

authorities play a vital role in safeguarding privacy rights. Their establishment and effective functioning contribute to a robust data protection ecosystem.

- **Addressing Cross-Border Data Flows**:

  Develop international agreements to facilitate cross-border data flows. Harmonise data protection standards globally. Adequacy decisions are formal determinations by the European Commission that a non-EU country provides adequate data protection. These decisions allow the free flow of personal data from the EU to the third country without additional safeguards. The EU-US Privacy Shield, previously considered an adequacy decision, was invalidated by the Court of Justice of the European Union (CJEU) in 20201. India can study the criteria used by the EU to assess adequacy and align its data protection framework accordingly. Standard Contractual Clauses (SCCs) are pre-approved contractual clauses that ensure appropriate data protection safeguards for international data transfers. The European Commission issued modernised SCCs under the General Data Protection Regulation (GDPR) in June 2021. These replace the previous sets of SCCs adopted under the Data Protection Directive 95/46. Organisations can use SCCs when transferring data from the EU/EEA to third countries lacking an adequate decision. Several countries and organisations worldwide have developed their model contractual clauses based on principles similar to those of the EU SCCs. Examples include the UK, Switzerland, and ASEAN2. Align India's data protection laws with EU standards to facilitate data transfers. Considering regional and sector-specific nuances, India can create its SCCs for cross-border data flows. Strengthen cooperation with international partners to enhance data transfers based on model clauses.

- **Regular Review and Adaptation**:

  The Act should evolve with changing technology and societal needs. Conduct periodic reviews to assess effectiveness and address emerging challenges. Involve stakeholders in the review process. Privacy by design is an approach that aims to protect individual privacy and data protection through intentional design choices. Design.[86]

[86] Cavoukian, A. (2019). Privacy by Design: The 7 Foundational Principles. Springer

In summary, the Digital Personal Data Protection Act 2023 is a significant step toward safeguarding privacy rights[4]. However, continuous monitoring, stakeholder engagement, and adaptive improvements are essential for its long-term success. In reflecting on our comprehensive exploration, it's evident that while the Digital Personal Data Protection Act 2023 represents a substantial step forward in safeguarding data privacy, particularly in wearable technologies, significant complexities are yet to be fully addressed. Our analysis has brought to light the multifaceted nature of privacy concerns related to wearable technology, amplified by the rapid evolution of these devices and the highly personal data they collect and handle.

The rapid advancement of technologies, especially wearable devices, highlights a significant gap in existing legal frameworks that were not designed to address the multifaceted challenges posed by modern digital technologies. This discrepancy underscores the imperative need for legislative bodies to adopt a more responsive and adaptive approach to regulation that can evolve with technological progress. The emphasis on incorporating specificity, robust privacy measures, data minimisation principles, and enhanced security standards suggests a move towards a more prescriptive change in the Digital Personal Data Protection Act 2023. The study's reference to the need for a collaborative protection effort highlights the importance of stakeholder engagement in this process. By involving technologists, users, and legal experts in drafting and revising the Act, policymakers can ensure that regulations are both technically feasible and socially beneficial. The comparison with global benchmarks, such as the GDPR, further highlights the significance of international collaboration and learning from the experiences of other jurisdictions. As technology increasingly transcends borders, the protection of digital privacy necessitates a harmonised approach that considers global standards and practices. This facilitates cross-border data flows and fosters a collective effort towards establishing a resilient framework against privacy risks.

. Establishing mechanisms for regular review and adjustments of legal frameworks is essential, ensuring they protect personal data effectively without stifling innovation. Ultimately, the study encapsulates a forward-thinking approach to legislative reform in the digital age. It calls for a balanced and proactive legal framework that anticipates future developments, engages diverse stakeholders, and aligns with international standards, all while safeguarding individuals' privacy rights. Achieving this balance is paramount in fostering a digital ecosystem that promotes innovation and respects privacy, paving the way for a more secure and privacy-conscious technological landscape.

BIBLIOGRAPHY

Statutes and Regulations

The Digital Personal Data Protection Act (DPDPA) 2023

General Data Protection Regulation (GDPR) 2016

Health Insurance Portability and Accountability Act (HIPAA) 1996

California's Consumer Privacy Act (CCPA) 2020

Information Technology (IT) Act, 2000

Constitution of India 1950

The Rights of Persons with Disabilities Act, 2016

Books and Articles

Shan, Li, and Chen Pei. "Internet of Things (IOT) Development for the Promotion of Information Economy," November 2015.

Khan, Saad, Simon Parkinson, Liam Grant, Na Liu, and Stephen Mcguire. "Biometric Systems Utilising Health Data from Wearable Devices." ACM Computing Surveys 53, no. 4 (July 11, 2020)

De Zambotti, Massimiliano, Nicola Cellini, Aimée Goldstone, Ian M. Colrain, and Fiona C. Baker. "Wearable Sleep Technology in Clinical and Research Settings." Medicine and Science in Sports and Exercise 51, no. 7 (February 19, 2019)

Haghi, Mostafa, Saeed Danyali, Sina Ayasseh, Ju Wang, Rahmat Aazami, and Thomas M Deserno. "Wearable Devices in Health Monitoring from the Environmental towards Multiple Domains: A Survey." Sensors 21, no. 6 (March 18, 2021)

Ferree, Thomas C, Phan Luu, Gerald S Russell, and Don M Tucker. "Scalp electrode impedance, infection risk, and EEG data quality." Clinical Neurophysiology 112, no. 3 (March 1, 2001):

Li, Guang-Li, Jing-Tao Wu, Yong-Hui Xia, Quan-Guo He, and Hong-Guang Jin. “Review of semi-dry electrodes for EEG recording.” Journal of Neural Engineering 17, no. 5 (October 1, 2020):

Wu, Ju-Yu, Congo Tak-Shing Ching, Hui-Min David Wang, and Lun-De Liao. “Emerging Wearable Biosensor Technologies for Stress Monitoring and Their Real-World Applications.” Biosensors 12, no. 12 (November 30, 2022

Ernst, Claus-Peter Hermann and Alexander W. Ernst. “The Influence of Privacy Risk on Smartwatch Usage.” Americas Conference on Information Systems (2016).

Kapoor, Vidhi & Singh, Rishabh & Reddy, Rishabh & Churi, Prathamesh. (2020). Privacy Issues in Wearable Technology: An Intrinsic Review. SSRN Electronic Journal. 10

Panayiotou, Andrie G., and Evangelos D. Protopapadakis. “Ethical issues concerning the use of commercially available wearables in children: Informed consent, living in the spotlight, and the right to an open future.” *JAHR* 13/1, no. No. 25 (2022).

Bouderhem, Rabaï. 2023. "Privacy and Regulatory Issues in Wearable Health Technology" Engineering Proceedings 58

Rosie Dobson et al., “Use of Consumer Wearables in Health Research: Issues and Considerations,” JMIR. Journal of Medical Internet Research/Journal of Medical Internet Research 25 (November 21, 2023).

“Privacy Data Ethics of Wearable Digital Health Technology,” Center for Digital Health | Engineering | Brown University, May 4, 2023

Khilansha Mukhija and Shreyas Jaiswal, “Digital Personal Data Protection Act 2023 in light of the European Union’s GDPR,” Jus Corpus Law Journal, November 7, 2023

Luisa Rollenhagen, “Alan Westin is the father of modern data privacy law,” Osano, January 15, 2021

F. H. Cate and V. Mayer-Schonberger, “Notice and consent in a world of Big Data,” International Data Privacy Law 3, no. 2 (May 1, 2013): 67–73, https://doi.org/10.1093/idpl/ipt005.

Anna Bruvere and Victor Lovic, “Rethinking Informed Consent in the Context of Big Data,” April 19, 2021

Neil C. Manson and Onora O'Neill, Rethinking Informed Consent in Bioethics, 2007

Anglano & C. Lipman (2022). When Anonymized Isn't Enough: Re-identification Risks in the Age of Wearable Technology. Santa Clara Law Review, 59(2), 521-558.

Paul Ohm, "Broken Promises Of Privacy: Responding To The Surprising Failure Of Anonymization," 57 Ucla Law Review, 2010

Muneeb -Ul-Hasan and Siti Hajar Othman, "A Conceptual Framework of Information Security Database Audit and Assessment," International Journal of Innovative Computing 9, no. 1 (May 31, 2019)

Mukhija, Khilansha, and Shreyas Jaiswal. "Digital Personal Data Protection Act 2023 in light of the European Union's GDPR." Jus Corpus Law Journal, November 7, 2023

Cynthia Jayapal et al., "Challenges in Wearable Technology," 2021 International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA), October 8, 2021

Khan, Saad, Simon Parkinson, Liam Grant, Na Liu, and Stephen Mcguire. "Biometric Systems Utilising Health Data from Wearable Devices." ACM Computing Surveys 53, no. 4 (July 11, 2020)

Garmin, "Privacy Policy" (Garmin, April 2022) accessed 23 May 2022. Also see: WS Wearable Stories, 'Privacy Statement' (WS, February 2021)

Jan Benedikt Brönneke et al., "Regulatory, Legal, and Market Aspects of Smart Wearables for Cardiac Monitoring," Sensors 21, no. 14 (July 20, 2021)

Rajakariar, K.; Buntine, P.; Ghaly, A.; Zhu, Z.C.; Abeygunawardana, V.; Visakhamoorthy, S.; Owen, P.J.; Tham, S.; Hackett, L.; Roberts, L.; et al. Accuracy of Smartwatch Pulse Oximetry Measurements in Hospitalized Patients with Coronavirus Disease 2019. Mayo Clin. Proc. Digit. Health 2024, 2, 152–158.

I. Glenn Cohen, "Informed Consent and Medical Artificial Intelligence: What to Tell the Patient?," The Georgetown Law Journal, vol. 108, 2020.

Sean Hooley and Latanya Sweeney, "Survey of Publicly Available State Health Databases," Social Science Research Network, January 1, 2013, https://doi.org/10.2139/ssrn.2277688.

Asma Sifaoui and Matthew S. Eastin, "'Whispers from the Wrist': Wearable Health Monitoring Devices and Privacy Regulations in the U.S.: The Loopholes, the Challenges, and the Opportunities," Cryptography 8, no. 2 (June 19, 2024)

Bennett Moses, L., & Chan, J. (2019). Data Trusts: Creating a Fair and Just Digital Economy. The Ada Lovelace Institute.

Miscellaneous

Cientifica Ltd (Publisher), April 2019, Report on 'Smart Textiles and Nanotechnologies: Appplications, Technologies and Markets', www.cientifica.com

News-Medical. "How do wearable fitness trackers measure steps?," April 7, 2023. https://www.news-medical.net/health/How-do-wearable-fitness-trackers-measure-steps.aspx. Accessed on 10th April 2024

Facebook, "Data policy," April 2018. [Online]. Available: https://www.facebook.com/ policy.php

Google, "Privacy policy," March 2020. [Online]. Available: https://policies.google.com/ privacy

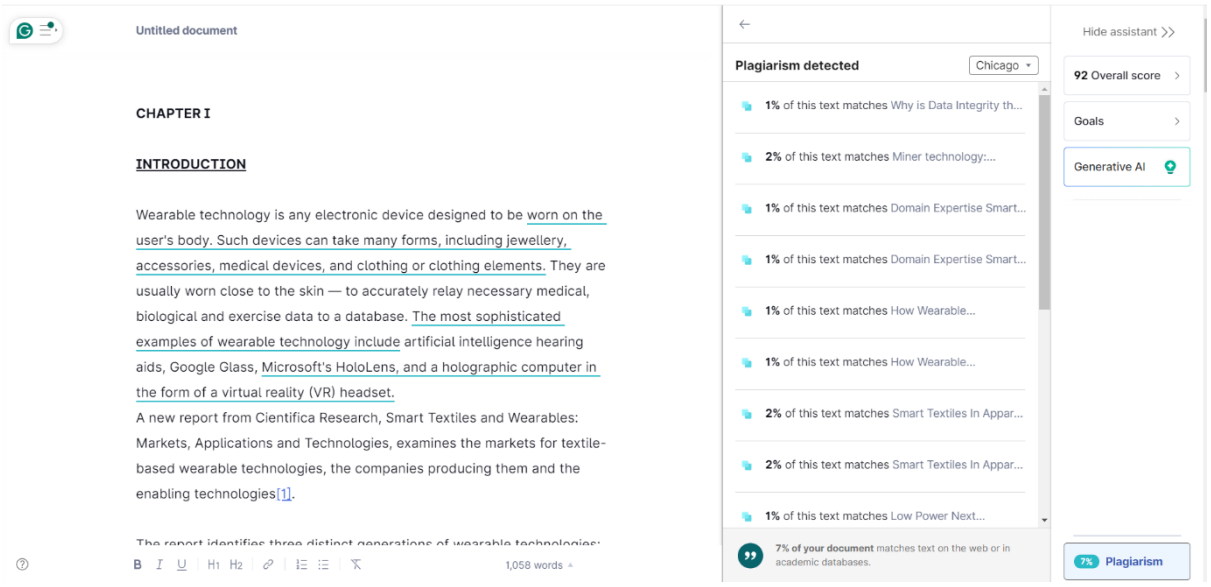
S. Inc., "Privacy policy," December 2019. [Online]. Available: https://www.snap.com/ en-US/privacy/privacy-policy

David Medine and Gayatri Murthy, "Companies, not people, should bear the burden of protecting data," Brookings, December 18, 2019, https://www.brookings.edu/articles/companies-not-people-should-bear-the-burden-of-protecting-data/. Accessed on 24th March 2024

Bamberger, K. A., & Mulligan, D. K. (2013). Privacy on the Ground: Driving Corporate Behavior in the United States and Europe. MIT Press.

APPENDIX

Chapter 1- 7%



Untitled document

CHAPTER I

INTRODUCTION

Wearable technology is any electronic device designed to be worn on the user's body. Such devices can take many forms, including jewellery, accessories, medical devices, and clothing or clothing elements. They are usually worn close to the skin — to accurately relay necessary medical, biological and exercise data to a database. The most sophisticated examples of wearable technology include artificial intelligence hearing aids, Google Glass, Microsoft's HoloLens, and a holographic computer in the form of a virtual reality (VR) headset.
A new report from Cientifica Research, Smart Textiles and Wearables: Markets, Applications and Technologies, examines the markets for textile-based wearable technologies, the companies producing them and the enabling technologies[1].

1,058 words

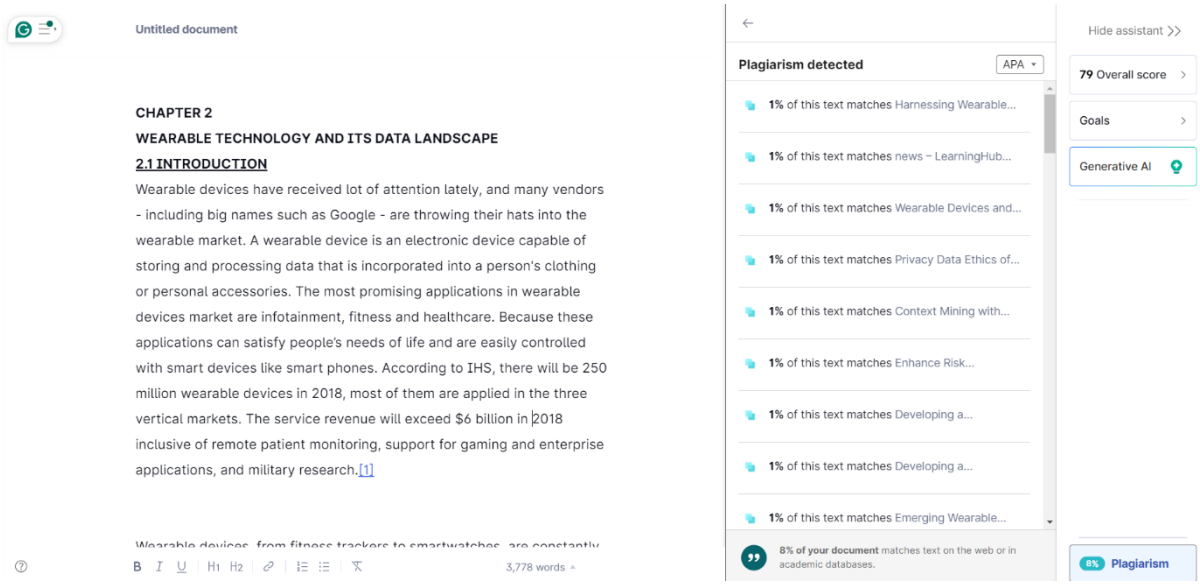
Plagiarism detected — Chicago

1% of this text matches Why is Data Integrity th...
2% of this text matches Miner technology:...
1% of this text matches Domain Expertise Smart...
1% of this text matches Domain Expertise Smart...
1% of this text matches How Wearable...
1% of this text matches How Wearable...
2% of this text matches Smart Textiles In Appar...
2% of this text matches Smart Textiles In Appar...
1% of this text matches Low Power Next...

7% of your document matches text on the web or in academic databases.

Hide assistant
92 Overall score
Goals
Generative AI
7% Plagiarism

Chapter 2- 8%



Untitled document

CHAPTER 2
WEARABLE TECHNOLOGY AND ITS DATA LANDSCAPE
2.1 INTRODUCTION
Wearable devices have received lot of attention lately, and many vendors - including big names such as Google - are throwing their hats into the wearable market. A wearable device is an electronic device capable of storing and processing data that is incorporated into a person's clothing or personal accessories. The most promising applications in wearable devices market are infotainment, fitness and healthcare. Because these applications can satisfy people's needs of life and are easily controlled with smart devices like smart phones. According to IHS, there will be 250 million wearable devices in 2018, most of them are applied in the three vertical markets. The service revenue will exceed $6 billion in 2018 inclusive of remote patient monitoring, support for gaming and enterprise applications, and military research.[1]

3,778 words

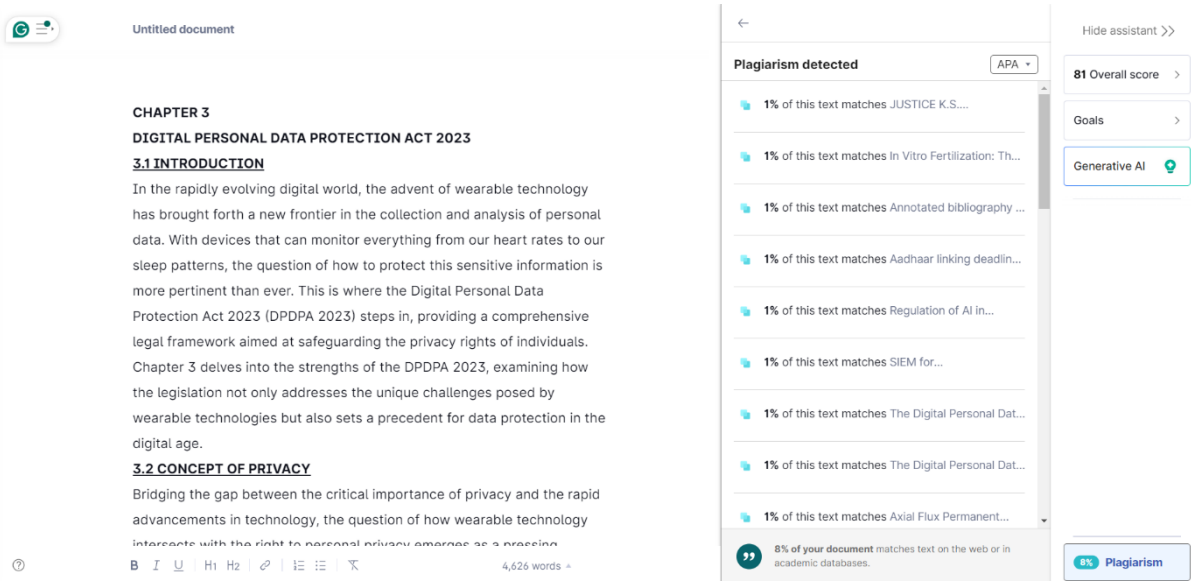
Plagiarism detected — APA

1% of this text matches Harnessing Wearable...
1% of this text matches news – LearningHub...
1% of this text matches Wearable Devices and...
1% of this text matches Privacy Data Ethics of...
1% of this text matches Context Mining with...
1% of this text matches Enhance Risk...
1% of this text matches Developing a...
1% of this text matches Developing a...
1% of this text matches Emerging Wearable...

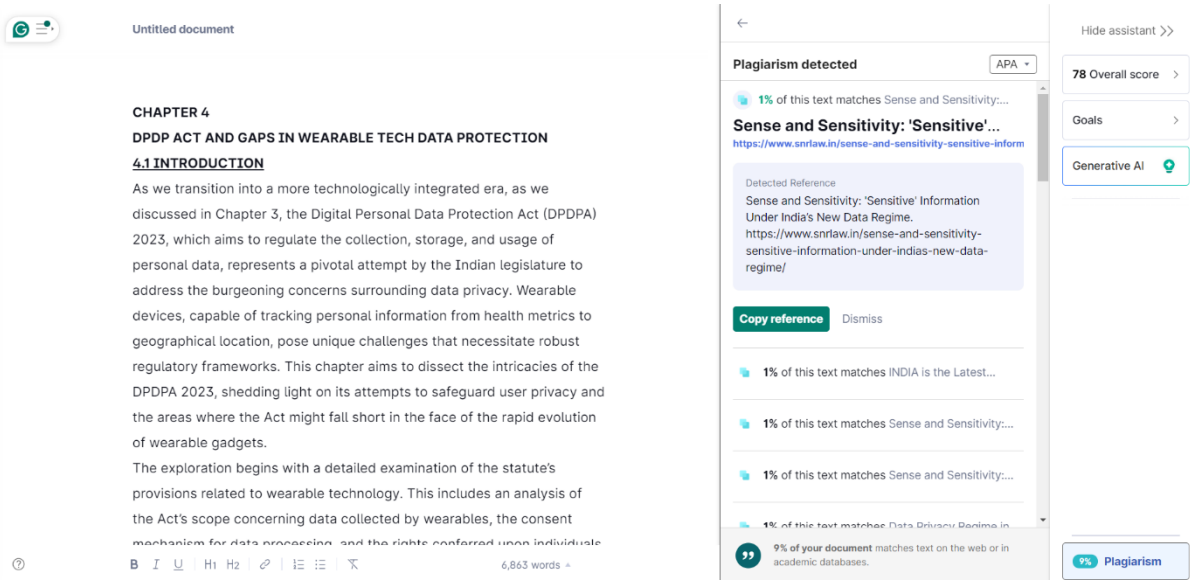
8% of your document matches text on the web or in academic databases.

Hide assistant
79 Overall score
Goals
Generative AI
8% Plagiarism

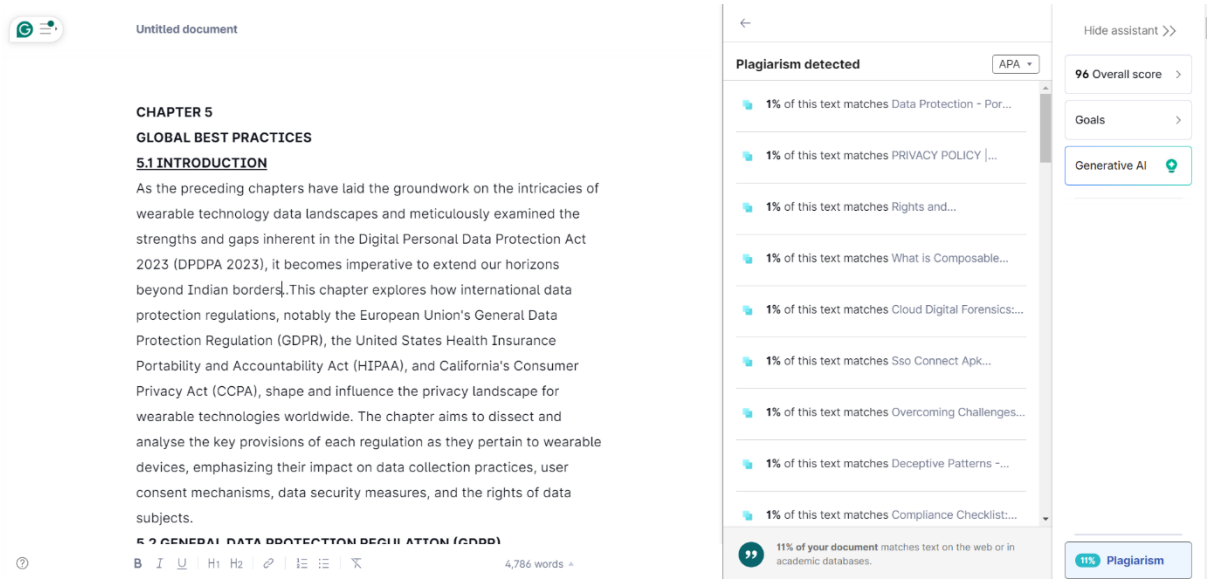
Chapter 3- 8%



Chapter 4- 9 %



Chapter 5- 11%



Chapter 6- 4%