Legal Information Management, 23 (2023), pp. 179–188

doi:10.1017/S1472669623000427

INTERNATIONAL PERSPECTIVES

Health Data on the Go: Navigating Privacy Concerns with Wearable Technologies

Abstract: The escalating adoption of wearable technology for health data monitoring has led to the real-time aggregation of personal information. This phenomenon has fuelled heightened apprehensions about data security and privacy, given the storage, processing, and sharing of personal health data by corporations. Regulatory frameworks have been enacted to safeguard individual privacy rights, as exemplified by the General Data Protection Regulation (GDPR). This research paper, by **Ms Varda Mone** and **Ms Fayazullaeva Shakhlo**, offers an overview of extant literature on privacy apprehensions concerning wearable devices, conducting an exhaustive review to discern pivotal privacy issues and proffer prospective remedies. Specifically, the paper delineates the ensuing privacy concerns associated with wearables. Predominantly, wearables introduce security vulnerabilities that may facilitate the misappropriation, compromise, or revelation of delicate health data. The copious health information amassed by wearables can be potentially sold or divulged to external parties' *sans* user cognisance or consent. Furthermore, the deployment of wearable technology harbours the potential for discriminatory practices against those with disabilities or chronic ailments. Additionally, apprehensions pertaining to privacy and surveillance stem from the capacity of wearable devices to monitor and trace an individual's movements and activities. To conclude, the paper deliberates on plausible measures to address privacy concerns pertaining to wearable devices, encompassing: a) Fortifying the security apparatus of wearable devices, b) Amplifying user autonomy over their health data, and c) Regulating the collection and utilisation of user health data by wearables. The paper asserts that the amelioration of these privacy concerns is indispensable for leveraging wearable technology's potential to enhance human well-being while ensuring the preservation of personal privacy.

Keywords: Data protection; General Data Protection Regulation (GDPR); Wearable Technologies; Internet of Things; Health Data

1. INTRODUCTION

The digital revolution in healthcare has led to a more accessible treatment system. The European Union (EU) and India have made significant strides in adopting digital health technologies, improving healthcare delivery, patient outcomes, and system efficiency. The EU has implemented electronic health record (EHR) systems, telemedicine services, health data exchange networks, digital health start-ups, and the National Digital Health Mission (NDHM). India has launched the National Health Stack, which includes Health ID, personal health records, telemedicine services, and electronic prescriptions. AI and data analytics are being explored to improve diagnostics, disease surveillance, and population health management. Remote monitoring and Internet of Things (IoT) devices are increasingly used in India for remote patient monitoring. However, data privacy, security concerns, legal frameworks, interoperability, and equitable access to digital health services remain challenges for both EU and India. Healthcare providers are working to address these issues and to utilise digital health to enhance patient care and results.[1]

Wearable technology refers to any electronic device that can be attached to the body in the form of clothing or accessories designed to perform a specific function. Although the idea of wearable technology has been around

https://doi.org/10.1017/S1472669623000427 Published online by Cambridge University Press

for a while, these devices did not become widely used and practical until recent technological advancements.[2]

The 'Manpo-kei' pedometer, invented in 1965 in Japan, was the first wearable fitness gadget. It was worn around the waist and counted steps through a mechanical mechanism. Although not as advanced as today's fitness trackers and smartwatches, it served as a significant precursor to more advanced devices. More recently, wearable technology has grown in popularity, with new products like smartwatches, fitness trackers, and virtual reality headsets entering the market every year. These gadgets offer various features, such as tracking physical activity, monitoring health, and improving entertainment.[3]

This research paper sheds light on the many sorts of data breaches experienced by a variety of companies. It found that hacking and information technology mishaps are the most common issues that led to breaches of healthcare data, followed by unauthorised internal disclosures. The number of data breaches in the healthcare industry, the volume of information exposed, and the monetary losses incurred as a result of these breaches are rapidly growing. There are serious privacy concerns with the use of wearable technologies to gather and share health data. We should think carefully before giving these devices access to our genetic information and medical histories as we entrust them with sensitive personal information.[4]

This paper discusses privacy concerns related to wearable technology for health monitoring and data collection. It examines the information collected, potential risks, and moral and legal guidelines. Solutions to address these issues include creating clear privacy policies, implementing encryption, and employing security measures to safeguard health data. Technology is increasingly being used in business, and businesses are increasingly using devices to track health, monitor productivity, personalise services, and provide data analytics. The internet offers these gadgets a platform for conducting online exchanges of information and providing people with different opportunities for interaction. Fitness trackers offer users access to activity tracking, heart rate monitoring, and other applications. The devices need to ensure that user privacy is always safeguarded, it is vital that the right security measures for protecting this kind of data are put into action. Users generally don't want a lot of security details, they would prefer it if their particular data was stored on secure servers that many different companies are using, however this can be an expensive option.[5] Cyber security is crucial for both workplace and home environments, ensuring safety, wellness, and cost-effectiveness. Companies must protect their devices from hackers and malicious personnel, and avoid connecting to hacked networks. Personal information protection is essential, and organisations often enforce strong password policies and strong password creation processes. It is essential for individuals to be cautious about their own accounts and to protect their personal information.

2. LITERATURE REVIEW

Authors Nedungadi, *et al* in the context of the Internet of Things, talk about worries about privacy, security and confidentiality. This review article explores the privacy and security concerns that have been raised in relation to the Internet of Things and wearable health devices. Unauthorised access to private medical records and cyber-attacks are also addressed.[6]

Wencheng Sun, *et al* authored a paper entitled 'Wearable Devices and Healthcare: Privacy and Information Security'. This article offers an in-depth analysis of the security and privacy issues surrounding wearable medical technology. Data sharing and secondary use, user consent and control, and the risk of data breaches and other unauthorised access to protected health information are all discussed.[7]

Tu, Jiaobing, and Wei Gao wrote 'Ethical Considerations of Wearable Technologies in Human Research'. This article is a review of the ethical and privacy issues that need to be thought through when creating wearable health devices. The authors argue that the potential benefits of these technologies outweigh privacy concerns, and they discuss topics like informed consent, data sharing and access, the need for transparency and accountability in the design and use of these devices, and so on.[8]

The article by Segura Anaya, LH, Alsadoon, A, Costadopoulos, N, and Prasad, PWC, is entitled 'Implications of User Perceptions of Wearable Devices. Science and Engineering Ethics.' This review article explores the privacy and security issues that arise with the use of wearable health devices and provides recommendations for resolving these issues. More user consent, data encryption, and secure data storage and transmission are also highlighted.[9]

These literature reviews are helpful because they give a broad perspective on the issues of privacy and security that surround the use of wearable health devices. They stress the need for informed consent from users, safe data storage and transmission, and increased openness and responsibility in the creation and management of such devices.

3. SECURITY AND PRIVACY ISSUES IN WEARABLES AND FITNESS TRACKING FROM A GDPR PERSPECTIVE

We construct our private lives on a foundation of physical distrust; we lock our doors, we don't flash our cash, and we steer clear of back alleys at night. Despite this, we tend to be less cautious when it comes to our personal information when we're online, often disclosing details about ourselves that we wouldn't otherwise expose because we believe that a password is enough to keep us safe. Sensitive information can easily escape the confines of conventional company networks due to the proliferation of cloud-based services and the growing popularity of mobile computing and the use of personal devices in

https://doi.org/10.1017/S1472669623000427 Published online by Cambridge University Press

the workplace. In fact, businesses that want to take advantage of cloud computing and the efficiency of 'bring your own device,' or BYOD, have implemented new policies and practices that give workers remote access to company data. This provides hackers with more opportunities to breach security. Social networking is often used by attackers in conjunction with other user mode assaults, such as spear phishing, to get access to a company's sensitive information by impersonating an employee. Therefore, companies put themselves in unnecessary danger when they provide staff access to more sensitive information than they need.

Healthcare data is becoming valuable for various purposes, including targeted marketing, illegal service acquisition and identity theft. Technological advancements offer both advantages and disadvantages in ensuring data privacy, security, accessibility, and identity authenticity. Cyber threats have become more complex and persistent, with weaker perimeter defences. However, the number of low-level attacks makes consumers more vulnerable, rather than the complexity of the attacks themselves. Even secure passwords are often insufficient in today's interconnected world. Data privacy in the European Union is governed by the GDPR, a sweeping piece of legislation. With the help of fitness tracking software and wearable technology, people can keep track of their fitness objectives, keep tabs on their health, and gather personal data.[10] However, there are potential GDPR privacy issues and vulnerabilities that must be handled in a legal, just and open manner. Data may be gathered from people outside the EU, and personal data breaches that cause unauthorised access to, disclosure of, or loss may occur. Organisational and technical safeguards must be in place to protect personal data from improper or unlawful processing by data controllers and processors.[11] Table 1 highlights the risks associated with the use of wearable gadgets, portable electronic devices, and mobile software by patients, medical institutions, and research entities within the healthcare industry. These risks are categorised under different scenarios and targets.

Table 1 shows that, overall, the adoption of wearable gadgets, portable devices and mobile software offers convenience and efficiency in the healthcare sector, but it also exposes patients, institutions, and research entities to a range of cybersecurity and data privacy risks. These risks highlight the importance of robust security measures, encryption protocols, and vigilant monitoring to safeguard sensitive patient information and research data.

4. IOT AND PRIVACY CONCERNS WITH DIGITAL BIOMARKERS AND SMART DEVICES

The widespread use of digital devices, such as wearables and smartphones, allows for the collection and analysis of vast amounts of user information as digital biomarkers. This can lead to personal significant findings for patients. However, sharing data and study findings can also lead to stigma and discrimination. To maintain trust, a data governance structure is crucial, involving donors, scientists, developers, healthcare service providers, and data and biobanks. Existing literature lacks positive data protection law considerations, despite suggestions for workable solutions. Incorporating digital biomarkers into psychiatric research creates a complex ecosystem, and GDPR legal requirements for controllers, processors, and joint controllers are discussed in the literature. The GDPR presents new challenges in the rapidly developing areas of wearable technology and the Internet of Things (IoT).[12]

An individual's location, biometric information, and health data can be collected by wearable technologies like smartwatches and fitness trackers. The same is true of the personal information collected by IoT devices like smart home gadgets, automobiles, and appliances.[13] According to the GDPR, organisations that collect this type of personal information have a greater responsibility to protect and responsibly handle it. Gaining permission before collecting and using a person's personal information is a major hurdle for wearable tech and IoT devices. According to the GDPR, an individual's consent for the processing of their personal data must be obtained in a transparent and understandable manner. This necessitates transparency on the part of organisations regarding the data they collect and why, as well as the provision of opt-out mechanisms for individuals whose data is being collected or processed.[14]

The bottom line is that businesses producing wearable tech or Internet of Things gadgets must ensure GDPR compliance. Companies have a responsibility to inform their customers about how they handle their personal information, gain their informed consent before collecting and using that information, and implement security measures to prevent unauthorised access to or loss of that information. Moreover, people should be able to view and change their own information.[15]

Overall, despite the fact that wearable technology has many benefits, it is crucial to address its drawbacks and legal ramifications in order to protect user data and privacy.[16] Coming back to the discussion on biomarkers, the use of digital biomarkers in research will inevitably lead to the collection and dissemination of copious amounts of sensitive individual information. The European Union's GDPR governs this type of data usage. The foundational principles for adhering to the GDPR are laid out in Article 5. This states that it is essential, first and foremost, that all data processing is done in a lawful, fair, and open fashion. Secondly, data must also be "collected for specified, explicit, and legitimate purposes, and not further processed in a way that is incompatible with those purposes" (the so-called purpose limitation principle). Thirdly, the 'data minimisation principle' dictates that only the bare minimum of information is gathered in order to achieve these ends. Similarly, the 'storage limitation principle' states that data may only be kept for as long as necessary to accomplish the

https://doi.org/10.1017/S1472669623000427 Published online by Cambridge University Press

Table 1: Potential security issues and risks involved with wearable tech and digital health data

Uses	Devices	Risks Involved
Universe: public Target: patients	Gadgets you can wear, portable electronic devices, and mobile software individual possession	1. Data breaches, identity theft, and unauthorised access to patient records or study results. Theft of personal information, identity theft, or unlawful access to research data or patient records. 2. Malware infection, device theft, or unauthorised access through social engineering are all potential causes of owner loss of control.
Universe: public Target: patients	Institutions, including medical centres and universities conducting research	1. Though somewhat lower than devices managed by organisation, there is still a risk of data compromise, identity theft, and unauthorised access to study results or patient information. 2. Due to device loss, social engineering, or malware infection, the owner may lose access to their device.
Universe: public Target: patients	Sending information from one place to another; with use of Bluetooth, Wi-Fi, Broadband	1. Denial of service, data modification undetected during transmission, and the interception of sensitive data in transit. 2. Lack of encryption, insecure transmission, or a broken encryption system. 3. Unauthorised access to study results or patient information, falsification of results, data loss/destruction, and theft of sensitive data are only some of the risks associated with doing research.
Universe: public Target: patients	Some examples of line-of-business applications are EHRs, personal health records (PHRs), web portals, research databases, analytics tools, and survey management systems for the healthcare industry. A mobile application market	1. Lack of timely audit or awareness; vulnerability to insider threat; inadequate cloud security; inadequate information technology security; insecure access for reporting study results (i.e., no protection against bots)

processing's stated goals. Data must be accurate and used securely, as outlined in Article 5(2) of the General Data Protection Regulation. According to the 'accountability principle', the burden of proof rests squarely on the data controller to demonstrate compliance with these requirements.

There are regulations governing the handling of medical and genetic information. Information about a person's health is considered 'special categories of data' (also known as 'sensitive data'). Article 9(1) GDPR states that such information must typically not be processed, unless an exemption from this rule is provided in Article 9.2. These exemptions are: expressed consent from the data subject; the data used is necessary for carrying out lawful non-profit activities; data used is necessary for performing lawful non-profit activities subject to appropriate safeguards; data subject makes data public; data processing is necessary for reasons of substantial public interest, including public health, as stated in an EU or Member State law that provides for appropriate safeguards. In order to protect the fundamental rights of the data subject, the data controller is responsible for evaluating whether any of these exemptions apply and for putting in place the necessary precautions.

Following the GDPR, data subjects are given a range of rights. According to Article 13 of the GDPR, data subjects in particular have the right to know the objectives and procedures of any processing of their personal data that affects them. Additionally, data subjects have the right to request a copy of the personal information that the controller has collected about them (Article 15 GDPR), to have any inaccurate information about them corrected (Article 16 GDPR), and to have any personal

https://doi.org/10.1017/S1472669623000427 Published online by Cambridge University Press

information collected about them erased (Article 17 GDPR) – for example, if the data subject withdraws their consent and there is no other legal basis for the processing. The use of data in scientific study is governed by a different set of laws. In this situation a few of the GDPR's data protection requirements may be disregarded. Article 5(1)(c) and (e) permits the keeping of personal data for longer than is necessary and the use of that data for research purposes other than the ones for which it was originally obtained. Derogations from the rights of data subjects to access, rectify, erase, and object are also anticipated by the GDPR: if the goals of the research would be rendered impossible or substantially impaired by the subject exercising one of their rights, the researcher may make an exception to the data subject's rights (Article 89(2) GDPR).

Exemptions for study, however, might only be permitted provided safeguards are put in place to protect "the rights and freedoms of the data subject" (Article 89 GDPR). The appropriateness, compliance, and to "ensure that technical and organisational measures are in place, in particular to ensure respect for the principle of data minimisation" of such safeguards are all requirements. The European Data Protection Board (EDPB) did provide some information on potential measures in the context of research even if Article 89 of the GDPR is silent on the matter.

The GDPR now governs international data transfers. If the European Commission issued a decision on adequacy recognising that the level of security in that country is appropriate under the GDPR, transfers of personal information to countries outside the EEA are permitted. Transfers may take place without any adequate determination provided the proper precautions are in place (Article 46 GDPR), such as standard contractual clauses, legally enforceable firm policies, authorised standards of conduct, or recognised certification procedures. To do this, the data supplier must initially map out the transfers, then choose the security measures to be used for the data transfer, then evaluate the laws of the destination nation with the help of legal experts, taking into account all data protection laws and actual practices in the third country, the ability of the authorities to access personal data for surveillance, and the presence of an effective right to judicial redress.

Data transfers may go ahead even in the absence of an adequacy determination and Article 46 protections if one of the exceptions in Article 49 of the GDPR applies. A pandemic, for instance, necessitates the particular consent of the data subject, the protection of the data subject's vital interests, and compelling public interest justifications. These exceptions must be read strictly, therefore no study can be stopped by relying on them.

5. PROFIT GAINING BY COMPANIES BY USING CONSUMER DATA

Selling consumer data for profit by fitness device manufacturers is a contentious practice that poses serious privacy issues. Companies that make wearable technology frequently gather a lot of user data, including private data that should not be shared, like biometric information, medical histories, and GPS location information. Third-party advertisers and other businesses may place a high value on this data, and they are frequently willing to pay sizable sums of money to obtain access to it.[17]

Lack of informed consent is one of the biggest privacy violations connected to the sale of consumer data by wearable technology companies. Many users might not be aware that their information is being gathered and sold, or they might not fully comprehend the potential dangers and consequences of this being done. Companies occasionally hide the specifics of data collection and use deep within their privacy policies, making it challenging for users to fully understand what is happening to their data.[18]

Users may suffer negative effects if wearable technology companies sell their customer data. By using this information, advertisers and marketers can target users with intrusive and unwanted advertisements and marketing materials. Additionally, it can be used to make decisions that have a significant impact on the lives of users regarding their employment, insurance and credit. Despite these worries, many companies that make wearable technology continue to make money by selling consumer data. It is vital for users to be informed of their rights to privacy and to vigilantly exercise that right in order to ensure that corporations are held responsible for any privacy violations.

From 2009 to 2022, 5150 healthcare data breaches affecting 500 or more records were reported to the US Office for Civil Rights of the Department of Health and Human Services (HHS), as shown in Figure 1. Because of these breaches, the protected health information of 382,262,109 patients has either been made public or disclosed in a manner that is prohibited. That is equivalent to more than one and a half times the population of the EU. On average, one healthcare data breach affecting 500 or more records was reported every day in 2018. After five years, the rate has more than doubled, as can be seen by looking at the data. There was an average of 1.94 healthcare data breaches affecting 500 records or more each day in 2022. Concern about the use of patient data by the pharmaceutical and insurance industries has grown in recent years. Even though the use of health data can enhance medical research and offer personalised healthcare, it also raises serious privacy concerns. In 2018, for example, fitness tracking app Strava came under fire when it was discovered that its 'heatmap' feature, which showed the running and cycling routes of users, had revealed potentially sensitive military locations. While this issue did not involve the sale of personal data, it highlighted concerns about the potential risks of sharing personal data through wearable technology.[19]

Pharmaceutical firms use health information to carry out clinical trials, create new medications and treatments, and locate potential consumers for their goods. However, there are questions regarding how this data is gathered, stored, and used. Additionally, health insurance companies

https://doi.org/10.1017/S1472669623000427 Published online by Cambridge University Press

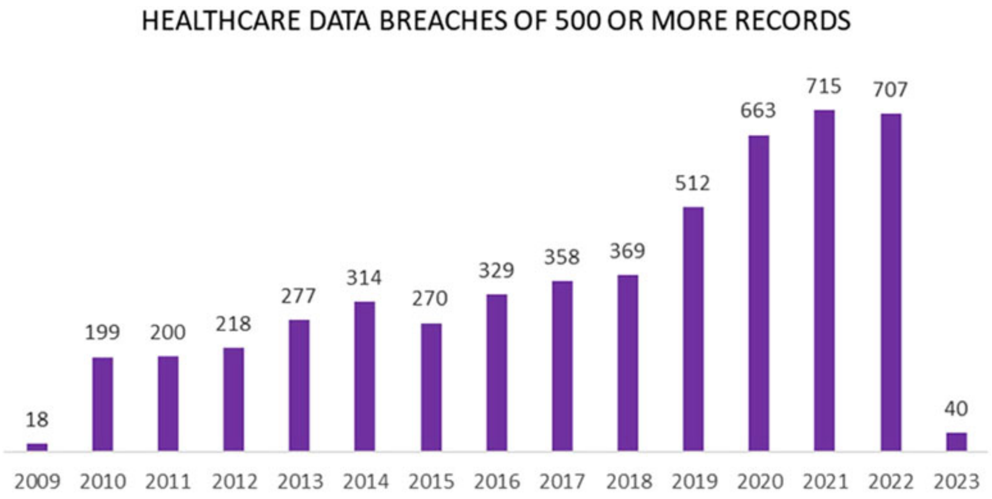

Figure 1: Healthcare data breaches from 2009-2023 (note, data incomplete for 2023)

use health data to determine the risk of covering a specific person, and change premiums as necessary. This practice can aid in ensuring that insurance providers are solvent and able to offer protection to their clients, but it can also be discriminatory and give rise to privacy concerns.[20]

Here are a few more instances in which personal information was compromised by fitness devices:

1. Concerned that smartwatches could be used to track the locations and movements of soldiers, the Dutch military issued a ban on their use in 2018. This was after a soldier accidentally revealed the location of a base while using a fitness tracking app on his smartwatch during a military exercise.[21]
2. *The Washington Post* conducted an investigation in 2019 that found that popular fitness tracking apps were disclosing menstrual cycles, pregnancy status and mental health information of users to third-party advertisers. It's possible that this data will be used for malicious purposes like targeted advertising.[22]
3. It was revealed in 2020 that the fitness tracking app MyFitnessPal had been the victim of a data breach that exposed the email addresses, usernames and hashed passwords of about 150 million users. The company discovered the breach in February of 2018, but did not announce it until much later.[23]
4. In 2021, a cybersecurity firm discovered multiple flaws in a widely sold children's smartwatch that could have allowed hackers to steal sensitive information or even track the wearer's location. Bluetooth connections could be compromised, and user information was not encrypted.[24]

Wearable fitness devices face privacy and security risks, requiring individuals to review policies and take necessary precautions. Companies must gather and use health data responsibly, obtain informed consent, implement strong security measures, and only use data for permitted activities. Regulatory bodies must establish clear guidelines and regulations to hold businesses accountable for privacy violations and motivate them to use health data for patient and societal benefits.[25]

6. DATA LOCALISATION CONCERNS FOR FITNESS TRACKER SECURITY AND PRIVACY

Wearable gear must prioritise data privacy and security, as many devices store sensitive health information without encryption, increasing the risk of disclosure. Third-party applications on wearable sensors can heighten vulnerability to data breaches. There are two types of attacks that can compromise data security on wearable devices: 'passive' and 'aggressive'. An Inertial Measurement Unit (IMU) is an electronic device that measures force, angular rate, and orientation of an object or body. IMU data, including accelerometers, gyroscopes, and magnetometers, can be obtained through wearable devices, which can be used to replicate confidential key inputs for electronic door locks and ATMs.

Wearable devices are causing concern among individuals regarding the confidentiality of their personal data. Fitness trackers record geocoordinates, but security concerns arise when cameras and microphones are integrated. Privacy is also threatened by wearable technologies. To improve data security and protection, consumers should understand the data collected by their devices and its consequences.

Alternative methods for security and privacy include using cryptographic techniques, using PINs to encrypt devices, opting for cloud storage, and using secure network interfaces for data transfer. These technologies minimise information loss. Fitness tracking devices have gained popularity for tracking fitness and health data, but they can also collect private data, posing security and privacy risks. Companies must consider data localisation when designing products and store personal information in secure locations, such as cloud providers with robust protocols, or in the same country as the user.[26]

https://doi.org/10.1017/S1472669623000427 Published online by Cambridge University Press

Fitness tracking device manufacturers must ensure encryption of personal information during transmission and storage, transparent data processing procedures, and user access to control. They should create devices from a data localisation perspective, ensuring secure and private processing and storage. By considering data localisation, encryption, and transparency, businesses can protect user privacy and ensure a secure and user-friendly experience.

The following are a few of the more important clauses that relate to wearable health devices:[27]

- Consent. The GDPR requires organisations to obtain an individual's authorisation before collecting and processing their personal data. To collect health data from consumers, companies developing and operating wearable health devices will need to obtain consent from those consumers. (Articles 6(1)(a) and 7 of the GDPR).[28]
- Companies that handle sensitive information, such as medical records, must have a legal basis for doing so under the GDPR. Companies running wearable health devices need to make sure they have a legitimate reason to handle personal health information. (Article 6(1)(f)[29] and Article 9[30] of the GDPR).
- Only the smallest amount of personal data necessary for a specific processing purpose shall be collected and maintained, as required by the GDPR. Therefore, it is crucial for companies that offer services associated with wearable health devices to make sure they only gather the least amount of health data required for the device's intended usage. (Article 5(1)(c) of the GDPR).[31]
- Individuals have rights under the GDPR, including being able to access their data, have any mistakes corrected, and have their data deleted if necessary. Businesses providing wearable health devices to customers should guarantee these protections for their customers. (Articles 15-22 of the GDPR).[32]
- The GDPR mandates that businesses take specific, quantifiable steps to protect the confidentiality, integrity, and availability of personal information. Wearable health device operators must take reasonable precautions to protect the privacy, authenticity, and accessibility of their customers' health information. (Article 32 of the GDPR).[33]
- Within 72 hours of becoming aware of a data breach, companies must notify the supervisory authority and any affected individuals. In order to comply with this mandate, businesses that offer wearable health devices should have robust data breach notification procedures in place. (Articles 33-34 of the GDPR).[34]

7. CHALLENGES AND LIMITATIONS OF GDPR IN WEARABLE HEALTH DEVICES

The main cause of privacy leaks is a lack of knowledge and adherence to best privacy practices and policies. Companies may not be transparent about their data collection and processing practices, and individuals may not be aware of the protections afforded by the GDPR. However, many wearable health devices and fitness apps rely on external service providers for data storage, processing and analytics, making it difficult to monitor and regulate data sharing. Companies have contracts in place to ensure these providers comply with the GDPR.[35]

Misplacing a wearable device or indiscriminately disclosing login credentials can lead to a privacy breach. Companies can help reduce the likelihood of these mistakes by providing training and information, but it is difficult to completely eliminate them. Inconsistent enforcement across the EU may lead to compliance gaps, so some businesses may opt to ignore the GDPR altogether.[36] Wearable health devices and fitness apps are rapidly developing, with new features and functionalities being released frequently. When adding new functionality, it can be difficult to test for and verify that it complies with the GDPR, especially if the functionality collects and processes personal data in ways that were not previously possible.[37]

The GDPR provides a thorough framework, but there are still openings that can be exploited to invade an individual's privacy. Increased awareness and education, improved data sharing agreements with third-party service providers, user training and guidance, consistent enforcement, and ongoing efforts to keep up with rapidly evolving technology are all necessary to address these gaps.[38] This paper has presented some background research on security and privacy related to wearable technologies. Overall, authentication problems are a significant threat. Therefore, additional research into authentication will be done in the future, and a better authentication system will be introduced.[39]

8. CONCLUSION AND SUGGESTIONS

In conclusion, wearable technology and fitness tracking programmes are governed by the GDPR and are required to follow its guidelines for safeguarding the personal data of users. This includes obtaining express consent before processing sensitive personal data, being transparent about the sharing of personal information with third-party service providers, and putting in place the necessary organisational and technical safeguards to protect personal information from loss or unauthorised access.[40]

The increasing prevalence of sophisticated dangers makes it impossible to predict when a threat will strike. The adoption of common applications and systems will drive attackers in the future decade. Privacy violations are primarily caused by a lack of knowledge about and adherence to appropriate safeguards. To address this, businesses should be more transparent about customer data collection and usage, and regulatory bodies can conduct public awareness campaigns to inform people about their rights and GDPR safeguards. Third-party service providers play a crucial role in the storage and processing of personal

https://doi.org/10.1017/S1472669623000427 Published online by Cambridge University Press

data in wearable health devices; therefore, improved data sharing agreements are necessary. A company can ensure its adherence to the GDPR by establishing comprehensive data-sharing agreements with its service providers. Auditing and monitoring for GDPR compliance may also be included in such agreements.[41]

Companies should educate users on safe wearable health device practices, such as strong passwords, avoiding public Wi-Fi, and two-factor authentication. User-friendly interfaces help manage data and privacy. GDPR enforces consistency across the EU, and breaches are reported to regulators. Periodic audits and data assessments ensure adherence to GDPR standards. Overcoming challenges requires awareness, education, robust agreements, training, strict enforcement, and continuous adaptation.

Footnotes

[1] Bajpai, Nirupam, and Manisha Wadhwa. India's National Digital Health Mission. No. 36. ICT India Working Paper, 2020.

[2] Metcalf, D., Milliard, S. T., Gomez, M., & Schwartz, M. (2016). Wearables and the internet of things for health: Wearable, interconnected devices promise more efficient and comprehensive health care. IEEE pulse, 7(5), 35-39.

[3] Marchant, G. (2020). The brain on your wrist: the legal implications of wearable artificial intelligence. Sci Tech Lawyer, 17(1), 16.

[4] Alharbi, R., & Almagwashi, H. (2019, August). The Privacy requirments for wearable IoT devices in healthcare domain. In 2019 7th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW) (pp. 18-25). IEEE.

[5] Manogaran, G., Thota, C., Lopez, D., & Sundarasekar, R. (2017). Big data security intelligence for healthcare industry 4.0. In Cybersecurity for industry 4.0 (pp. 103-126). Springer, Cham.

[6] Nedungadi, P., Jayakumar, A. & Raman, R. Personalized Health Monitoring System for Managing Well-Being in Rural Areas. J Med Syst 42, 22 (2018). https://doi.org/10.1007/s10916-017-0854-9

[7] Wencheng Sun, Zhiping Cai,Yangyang Li,Fang Liu,Shengqun Fang,and Guoyan Wang (2018) "Security and Privacy in the Medical Internet of Things: A Review", Secureity and Communication Networks, Hindawi.

[8] Tu, Jiaobing, and Wei Gao. "Ethical considerations of wearable technologies in human research." Advanced healthcare materials 10.17 (2021): 2100127.

[9] Segura Anaya, L. H., Alsadoon, A., Costadopoulos, N., & Prasad, P. W. C. (2018). Ethical implications of user perceptions of wearable devices. Science and engineering ethics, 24, 1-28

[10] Ferreira, J. J., Fernandes, C. I., Rammal, H. G., & Veiga, P. M. (2021). Wearable technology and consumer interaction: A systematic review and research agenda. Computers in human behavior, 118, 106710.

[11] Brönneke, J. B., Müller, J., Mouratis, K., Hagen, J., & Stern, A. D. (2021). Regulatory, legal, and market aspects of smart wearables for cardiac monitoring. Sensors, 21(14), 4937.

[12] Parziale A, Mascalzoni D. Digital Biomarkers in Psychiatric Research: Data Protection Qualifications in a Complex Ecosystem. Front Psychiatry. 2022 Jun. doi: 10.3389/fpsyt.2022.873392.

[13] Williams, P. A., & McCauley, V. (2016, December). Always connected: The security challenges of the healthcare Internet of Things. In 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT) (pp. 30-35). IEEE.

[14] Chawla, N. (2020). AI, IOT and wearable technology for smart healthcare? A review. Int J Green Energy, 7(1), 9-13.

[15] Hiremath, S., Yang, G., & Mankodiya, K. (2014, November). Wearable Internet of Things: Concept, architectural components and promises for person-centered healthcare. In 2014 4th International Conference on Wireless Mobile Communication and Healthcare-Transforming Healthcare Through Innovations in Mobile and Wireless Technologies (MOBIHEALTH) (pp. 304-307). IEEE.

[16] Karunarathne, S. M., Saxena, N., & Khan, M. K. (2021). Security and privacy in IoT smart healthcare. IEEE Internet Computing, 25(4), 37-48.

[17] Minbaleev, A. V., Nikolskaia, K. Y., & Zhernova, V. M. (2020, December). Legal Enforcement of Cybersecurity of Wearable Mobile Devices in Healthcare. In 2nd International Scientific and Practical Conference on Digital Economy (ISCDE 2020) (pp. 674-678). Atlantis Press.

[18] Alvarez, S. L., Baller, S. L., & Walton, A. (2021). Who Owns Your Health Data? Two Interventions Addressing Data of Wearable Health Devices among Young Adults and Future Health Clinicians. Journal of Consumer Health on the Internet, 25 (1), 35-49.

[19] Anne T. McKenna, Amy C. Gaudion, and Jenni L. Evans, The Role of Satellites and Smart Devices: Data Surprises and Security, Privacy, and Regulatory Challenges, 123 Penn St. L. Rev. 3 (2019)

[20] Mahajan, N., Garg, S., Pandita, S., & Sehgal, G. (2022). Smart Healthcare and Digitalization: Technological and Cybersecurity Challenges. In Cross-Industry Applications of Cyber Security Frameworks (pp. 124-147). IGI Global.

[21] <https://apnews.com/d29c724e1d72460fbf7c2e999992d258/Pentagon-restricts-use-of-fitness-trackers,-other-devices?utm_source=Twitter&utm_medium=AP_Politics&utm_campaign=SocialFlow> (Accessed on 11 Jan 2023)

[22] <www.washingtonpost.com/technology/2022/09/22/health-apps-privacy/> (Accessed on 15 Dec 2022)

[23] <www.theverge.com/2018/3/29/17177848/under-armour-myfitnesspal-data-breach-150-million-accounts-security> (Accessed on 25 Jan 2023)

https://doi.org/10.1017/S1472669623000427 Published online by Cambridge University Press

[24] <www.zdnet.com/article/security-flaws-in-childrens-smartwatches-make-them-vulnerable-to-hackers/> (Accessed on 11 Nov 2022)

[25] Lachman, K. (2019). Smart healthcare systems, wearable sensor devices, and patient data security. American Journal of Medical Research, 6(1), 43-49.

[26] Krajcsik, J. R. (2022). The State of Health Data Privacy, and the Growth of Wearables and Wellness Apps (Doctoral dissertation, University of Pittsburgh).

[27] Ioannidou, I., & Sklavos, N. (2021). On general data protection regulation vulnerabilities and privacy issues, for wearable devices and fitness tracking applications. Cryptography, 5(4), 29.

[28] Art. 7 GDPR: Conditions for consent <https://gdpr-info.eu/art-7-gdpr/>

[29] Art. 6(1)F "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."

[30] Art. 9 GDPR: Processing of special categories of personal data <https://gdpr-info.eu/art-9-gdpr/>

[31] Art. 5 GDPR: Principles relating to processing of personal data <https://gdpr-info.eu/art-5-gdpr/>

[32] Chapter 3 GDPR: Rights of the data subject <https://gdpr-info.eu/chapter-3/>

[33] Art. 32 GDPR: Security of processing <https://gdpr-info.eu/art-32-gdpr/>

[34] Art. 33 GDPR: Notification of a personal data breach to the supervisory authority <https://gdpr-info.eu/art-33-gdpr/>

[35] Jayapal, C., Shree, S. K., Kumar, R. L., & Muthukumar, S. (2021, October). Challenges in Wearable Technology. In 2021 International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA) (pp. 1-6). IEEE.

[36] Jhajharia, S., Pal, S. K., & Verma, S. (2014). Wearable computing and its application. International Journal of Computer Science and Information Technologies, 5(4), 5700-5704.

[37] Schukat, M., McCaldin, D., Wang, K., Schreier, G., Lovell, N. H., Marschollek, M., & Redmond, S. J. (2016). Unintended consequences of wearable sensor use in healthcare. Yearbook of medical informatics, 25(01), 73-86.

[38] Sridhar, A. P., PV, L., & Mohana, T. K. (2020). Wearable Devices in Healthcare 4.0: Effects, Trends and Challenges.

[39] Kapoor, V., Singh, R., Reddy, R., & Churi, P. (2020, April). Privacy issues in wearable technology: An intrinsic review. In Proceedings of the International Conference on Innovative Computing & Communications (ICICC).

[40] Sam, M. F. M., Ismail, A. F. M. F., Bakar, K. A., Ahamat, A., & Qureshi, M. I. (2022). The Effectiveness of IoT Based Wearable Devices and Potential Cybersecurity Risks: A Systematic Literature Review from the Last Decade. International Journal of Online & Biomedical Engineering, 18(9).

[41] Ioannidou, I., & Sklavos, N. (2021). On General Data Protection Regulation Vulnerabilities and Privacy Issues, for Wearable Devices and Fitness Tracking Applications. Cryptography, 5(4), 29.

Biographies

Ms Varda Mone graduated (B.A.LLB) from Nagpur University and has a post-graduation qualification (LLM in Constitution and Administrative Law) from Dr Ram Manohar Lohia National Law University, Lucknow. She has worked as an Assistant Professor at the Indore Institute of Law, Indore, MP for one year. She worked as a full-time research intern at the Office of Mr Vijay Sai Reddy, a Member of the Rajya Sabha, Indian Parliament. She has been selected for an International Research Fellow in Humanities and Social Sciences (Remote) by the University of Religions and Denominations (URD). She is a PhD Research Scholar at VIT-AP School of Law, VIT-AP University, pursuing a full-time PhD in Data Protection Law. Presently she is designated as an International Research Fellow at Tashkent State University of Law and can be contacted at vardamone52@gmail.com.

Ms Fayazullaeva Shakhlo has completed her Bachelor's degree and Master's degree (LLM in International Commercial Law) at Westminster International University in Tashkent. She has worked as an associate professor at the National University of Uzbekistan for a year. She also has been a member of a working group on the accession of the Republic of Uzbekistan to the WTO on behalf of the Competition and Consumer Protection Committee. She is an associate professor in the faculty of International Law and Human Rights at the Tashkent State University of Law and can be contacted at shakhlofayzullayeva777@gmail.com.

https://doi.org/10.1017/S1472669623000427 Published online by Cambridge University Press