International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

# Impact of Fashion Body-Measuring Devices on Cybersecurity

**Dhruvika Saini**

Independent Researcher (12th Grade Student), Heritage Xperiential Learning School, Gurugram, Haryana, India

**Abstract**

The fashion industry is now taking a totally different dimension with the invention of digital body-measuring devices through 3D scanning, AI, and machine learning for more accurate human body measurements. This technology facilitates personalized clothing and medical clothing creation, improves comfort and usability, and initiates future advancements in wearable technology for digital health. The exponential market growth in the category of digital health wearables (from $15.4 billion in 2020 to over $71.91 billion in 2023), highlights greater needs for tailored fashion and health with wearable digital health technologies. However, the advancement of this technology also presents ethical and cybersecurity threats, especially around privacy of data, algorithmic bias, informed consent, and potential abuse of sensitive personal data. Therefore, the precise use and measurement of user data, as well as sociocultural bias, should be more highly regulated and art regulated with transparency and visibility. In this light, cybersecurity, ethical principles, and consumer trust take absolute precedent and should be first order of concern for all stakeholders and involved parties in the global apparel market, projected at over $2.25 trillion by 2026. This paper will explore the technological progression of digital body measurement tools in fashion technology, the benefits of these technologies, the risks to cybersecurity and ethics, the regulatory landscape, and risk mitigation strategies, along with a discussion of trends regarding sustainability and digitalization.

**Keywords:** Digital Body Measurement, Fashion Technology, AI in Fashion, Data Privacy Cybersecurity Risks, Ethical Considerations, Algorithmic Bias

## 1. Summary

Digital body-measuring devices are an innovative development within fashion technology, whereby 3D scanning, AI, and ML are applied in identifying human body measurements with high accuracy. These further provide ample opportunities for the fabrication of tailor-made apparel and medical clothes that ensure better comfort and functionality for the user. [1][2]. In the wake of this soaring demand for wearable digital health technology, when the market value increased from $15.4 billion in 2020 to approximately $71.91 billion in 2023, the importance of these tools to improve health outcomes and personalize fashion became more emphasized. [1] Despite their huge potential benefit, the adoption of digital body-measurement, such tools create serious ethical and cybersecurity concerns. Collecting and storing sensitive personal health information opens up the risks of data breach and unauthorized access, raising growing demands for improved data privacy and increased manufacturer accountability [1][2]. In addition, it raises ethical concerns related to the accuracy of the measured values, potential misuse of such sensitive data, and the biased nature of algorithmic processing itself-all part of an increasingly complex tapestry requiring critical consideration and thoughtful regulation [3]. The risk of misrepresented data due to inaccurate measurements, coupled with difficulty in guaranteeing proper scanning conditions, serves to further increase user vulnerabilities. Issues of ownership and consent, therefore, make the ethical issues more complex since it is often the case that users have very little control over how their data is handled by corporations owning the measurement technologies. With more fashion brands using these tools, serious questions about algorithmic bias and discrimination in health monitoring contexts are developing some pretty deep sociocultural consequences that need to be discussed. Looking ahead, the crossroads of technology, ethics, and cybersecurity will define the future in fashion technology. With the global apparel market expected to surpass $2.25 trillion by 2026, all stakeholders will have to make the implementation of strong cybersecurity measures and ethical guidelines a priority to protect consumer data and earn the public's trust while navigating an ever-changing landscape. [6][7]

## 2. Background

The digital body measurement tools, considered one of the key innovations in the fashion technology industry, have utilized advanced technologies like 3D scanning, AI, and ML in measuring the accurate dimensions of the human body. These tools provide the possibility to make custom-fit medical garments and apparel, ensuring both comfort and functionality for the user [1][2]. As these technologies become more mainstream, the market for wearable digital health technology has similarly grown from a valuation of $15.4 billion in 2020 to an estimated $71.91 billion in 2023, a testament to the increased demand for devices that track and improve health outcomes [1]. Yet with great benefits also come very significant ethical and cybersecurity concerns. With increasing dependency on digital tools for measurement of the body, there is a significant hike in data privacy and security issues. Wearable devices often store sensitive personal health information that, when not well secured, is quite vulnerable to breaches and unauthorized access. Moreover, third-party use of data also poses other ethical concerns, thus creating the urge for manufacturers and developers of such technologies to be more transparent and accountable [1][2]. Ethical implications associated with body measurement applications are indeed many, including the accuracy of the measurements to the misuse of personal data. The proper light and background during scanning are among the challenges to be met by users of such technologies, as inaccuracies could mean misrepresentation of body dimensions [3].[4] With the inclusion of smart textiles and the development of digital fashion technologies, the complexity continues to increase. There is an even greater need for inclusive and diverse design practices for the different consumers' body shapes and sizes [6].[8] The soaring adoption of digital solutions within the fashion industry will necessarily drive security concerns focused on consumer data protection, trust, and experiences. The projected global apparel market will reach over $2.25 trillion by 2026; such intersecting spaces of technology, ethics, and cybersecurity will be very important in molding the future of fashion technology to its various impacts on consumer experiences and health outcomes [7][6].

## 3. Cybersecurity risks

The integration of digital body measurement tools in fashion technology presents huge risks regarding cybersecurity that can affect businesses and consumers alike. While fashion brands are increasingly using such technologies to improve customer experience, this increases the chance for potential cyber threats.

### 3.1. Data Breaches and Privacy Concerns

Many digital body-measuring tools represent a category of devices that usually collect sensitive personal information, such as biometric data. These raise significant data-privacy concerns. If unauthorized access or misuse of information occurs, serious ethical issues may emerge, involving violations of confidentiality and even identity theft.[9][5]. One such survey in 2023 pointed out that 85% of consumers would not interact with any company that is perceived to have weak security practices. It shows that cybersecurity measures are needed to maintain consumer trust [10].

### 3.2. Vulnerabilities in Loyalty Programs

Fashion brands typically operate extensive customer loyalty programs, collecting a vast amount of personal and purchasing data. These make for very attractive targets for cybercriminals, who will quickly take advantage of weaknesses and leak sensitive information either for identity theft or resale on the dark web [11]. It follows, therefore, that brand equity erosion from data breaches involves not just short-term financial losses but the loss of long-term customer relationships and loyalty.

### 3.3. Intellectual Property Theft

The fashion industry is heavily reliant on innovation and design secrecy. Cyberattacks on design files and pre-release information give competitors an unfair advantage and may jeopardize a brand's market position. Similarly, it's important to protect the intellectual property of sustainable innovations; a breach involving sensitive data about new eco-friendly technologies could hold back wider industry adoption of sustainable practices [11][12].

### 3.4. Ransomware Threats

Ransomware attacks will result in serious manufacturing and retail disruptions in the fashion sector. These attacks can disrupt production and retail operations, creating significant financial impacts and brand reputation damage [11]. This is also because modern fashion supply chains have become so digitally connected that one breach may affect multiple players.

### 3.5. Ethical Considerations and Data Ownership

Data ownership is the complicating factor in the ethical landscape of digital body-measurement tools: while users create data through their bodies, it is often corporations that own the devices or platforms collecting such information. Thus, tension about data rights and user consent can easily arise [5]. Transparency in data practices by brands, therefore, is required for building trust when it comes to consumer concerns in the usage of data and privacy rights [13].

## 4. Ethical Risks

The integration of digital body-measurement tools in fashion technology raises serious ethical concerns, primarily about data privacy, informed consent, and the potential for biased collection and use of data. As wearable technologies become increasingly common, it is important that ethical considerations regarding their deployment are carefully considered.

### 4.1. Data Privacy and Informed Consent

One of the major ethical issues is the gathering, storage, and utilization of personal information that is of a sensitive nature. Severe ethical concerns regarding privacy have arisen due to unauthorized access and misapplication of data, especially in respect to awareness by users of how their data will be utilized.[14][9] In the case of wearables, informed consent is even more complex due to the continuous and often passive nature of data collection. Traditional consent models, normally involving very lengthy and sometimes incomprehensible privacy policies, often fail at effectively ensuring users understand the extent of data being collected or how it might be used. [1]Given these limitations, there is a call for user-centered consent mechanisms, including just-in-time consent, whereby notifications of access to data pop up contextually when it is collected, and layered privacy information so that users can engage with key information without being confronted by legal heaping. [5] Moreover, dynamic consent management can be used to directly enable the control of users over their data, sharing settings, and revocation of consent. [5]

### 4.2. Data Ownership and User Rights

The question of data ownership complicates the ethical landscape of wearable technologies: even though users generate data through bodily activities, in most cases, devices that collect this data are owned by corporations, which raises tensions regarding the right to control data and related ownership rights. [15] Ethically, a strong case can be made for user-centric ownership of data, favoring users' rights to access their information in portable format and to decide how this data is used.

### 4.3. Bias and Fairness

Another critical ethical concern involves bias in algorithms that process data from wearables. The training data used may lead to skewness in the predictions, failing to represent all demographics. For example, when a training dataset is dominated by data from younger individuals, wearables may perform poorly for older populations. [16] That problem is further exacerbated by algorithmic biases that create non-neutral or even discriminatory outcomes, especially in sensitive fields like health monitoring.[16] Real-world examples include differences in heart rate monitoring and estimation of calorific counts, using skin tone and basal metabolic rates that can result in large inaccuracies and discrimination.[16] However, such biases affect not only individual users but also have broader societal implications in the way they reinforce existing inequalities.

### 4.4. Surveillance and Social Sorting

Wearable data are likely to enable mass surveillance and social sorting, raising profound ethical issues. The wearables gather personal information that could allow new forms of discrimination based on data profiles, hence contributing to social stratification and erosion of privacy.[5]This aspect of dataveillance also carries the risks of manipulation of individuals and whole populations, and so it is important to pay close consideration to how data are collected and used in the fashion technology industry.

## 5. Regulations and Compliances

### 5.1. Data Protection Legislation

The emergence of digital body measurement tools in the fashion industry calls for strong regulations on consumer privacy. Laws like the General Data Protection Regulation in Europe and the California Consumer Privacy Act in the United States establish an important framework for data protection. These laws grant rights to consumers over their personal information, and no such collection or sharing shall be done without obtaining explicit consent from them.[17][13] Yet, despite these regulations, the implementation remains inconsistent, loopholes persist, and companies have several ways to circumvent them. This has raised a demand for stricter and more consistent implementation of data protection laws.[13][18].

### 5.2. Industry Best Practices

Due to the increasing concerns over privacy, the fashion industry has begun promoting a corporate best-practices model to address its own issues before heavy government regulation is warranted. Firms should enact principles of privacy-by-design where security measures are integrated into the design phase of a product rather than implemented later in the life cycle of the product line [18]. This model has gained broad support from various stakeholders, including privacy advocates, due to the need for timely solutions within an evolving technological landscape [18]

### 5.3. Ethical Considerations and Compliance Challenges

The overlap between digital fashion and data privacy is riddled with ethical dilemmas. Fashion companies often collect detailed data related to the behavior, preferences, and body measurements of users, which could lead to targeted advertising but at the same time poses risks of misuse or unauthorized sale of personal information. [19] While algorithms and artificial intelligence systems provide increasing insights into fashion decisions, they are also beginning to raise concerns about bias and discrimination. These algorithms may have been developed from biased data or alternatively provide recommendations and pricing strategies that reflect existing societal inequalities [19]. It also calls for an interdisciplinary approach and international cooperation in developing regulatory frameworks that can address such complex issues. The difficulty is providing regulations safeguarding individuals while encouraging innovation and ethical practices within the fashion industry[20][16]. Without due oversight, digital body-measurement tools' risks could undermine the consumers' trust and the commitment to responsible practices by the industry [16][19].

## 6. Mitigations Strategies

In order to mitigate the cybersecurity and ethical risks related to digital body-measurement tools in fashion technology, several different strategies should be employed, such as robust cybersecurity practices, ethical considerations, and improved trust on the part of consumers.

### 6.1. Cybersecurity Measures

Only good cybersecurity can help protect sensitive data related to body measurement tools. This may involve multi-factor authentication to improve user verification procedures, as well as regular audits to detect system vulnerabilities [6][21]. Secondly, full encryption of data has to be carried out in order to prevent unauthorized access to user information, considering the serious threat of data breaches regarding consumer loyalty programs and design data [11][12]. Training of staff is another vital component of a cybersecurity strategy. Since human error is often the weakest point in a security setup, training employees to recognize phishing emails and the importance of protecting data can go a long way in reducing the risks of utilizing digital tools [6]. Incident response plans should be developed so that the organization can take immediate action in case of any data breach to reduce the impact of such threats and minimize damage to user data [6].

### 6.2. Ethics and Accountability

As digital body measurement increasingly depends on the functionality and decision-making of AI systems, there is a growing need to conceptualize ethical guidelines and mechanisms of accountability. A need thus exists to develop frameworks of accountability for possible algorithmic outcomes that may reflect bias or have negative social consequences to build trust in such technologies [20]. Besides, embedding transparency and principles of responsible AI use within the design and implementation of new body-measuring tools can contribute to making such innovation compatible with higher-order sustainability goals by limiting possible adverse impacts on consumer behavior and the environment [20].

### 6.3. Consumer Confidence

In an increasingly skeptical environment of corporate claims, consumer trust has to be fostered. Brands need to make radical transparency the golden standard, with clear and verifiable disclosures concerning data usage and security practices associated with body measurement tools. This could range from blockchain as an essential tool in the authentication of supply chain data to showing in real-time how the consumer's personal information is being used. In summary, with data protection and ethical concerns very high among consumers, being competitive in the market includes guaranteeing data protection and ethical behaviors. By adopting these mitigation strategies, fashion brands will have taken steps toward mitigating the complex cybersecurity and ethical risks that come with digital body measurement tools and can ensure the protection of consumer data while fostering a more sustainable and responsible industry.

## 7. Future Trends

The future of fashion will be very different because of the advanced technologies that will be integrated, sustainable projects, and a change in consumer expectations. By 2026, this industry is expected to alter its relations with clothing using required sustainability and circularity practices, increasingly considered a strategic priority by forward-thinking brands [6]. While just a few fashion executives currently see sustainability as a business-critical risk, consumer behavior does show a decisive shift: 71% of shoppers want to keep their clothes longer [6].

### 7.1. Technological Innovations

The role of technology, especially in AI and the process of digital transformation, is going to become increasingly crucial for the fashion sector. AI-powered forecast tools, such as Heuritech, will be crucial in enabling brands to stay competitive in an increasingly fast-moving market [6]. These technologies will not only drive agility in responding to trends but also enhance transparency and personalization of consumer experiences.

### 7.2. Consumer Behavior

With the resale market expected to boom to $350 billion by 2028, brands are going to have to shift gears to deliver on the circular fashion solutions that customers have come to expect [6]. It involves the adoption of technologies that might help raise awareness, enhance transparency, and facilitate accountability along the value chain. The way into an inclusive, personalized fashion experience will be driven by digital body measurement applications and other innovative solutions, and it is going to be key in driving loyalty and satisfaction among consumers [22][23].

### 7.3. Cybersecurity Considerations

With the rapid adoption of digital tools in fashion, cybersecurity risks will become a prominent concern. Integration of 3D body scanning and AI will raise significant cybersecurity concerns about the protection of consumer data to maintain trust [24][25]. Where digital transformation is increasingly taking over in this industry, legal and regulatory innovation to address such challenges will also be highly required [18].

### 7.4. Environmental Impacts

Although digital fashion creates opportunities for waste reduction and increased efficiency, there are also energy consumption and electronic waste concerns. The environmental cost of digital technologies' energy demands needs to be very carefully managed, so as not to outweigh benefits accrued from avoidance of physical production. Moving forward in such complexities, it will be instrumental in the alignment of technology and sustainability with ethical practice for the realization of a future that is beneficial to both people and the planet.

## References

1. A. Spuskanyuk, "Ethical Implications of Wearable Digital Health Technology: Balancing Innovation and Patient Autonomy", American Journal of Healthcare Strategy, 2024.

https://ajhcs.org/article/ethical-implications-of-wearable-digital-health-technology-balancing-innovation-and-patient-autonomy
2. MobiDev, "Guide to Building AI-Powered 3D Body Measurement Applications", MobiDev Blog,https://mobidev.biz/blog/ai-body-measurement-application-development-guide
3. MirrorSize, "Body Scanning Technology for Apparel", MirrorSize Blog. https://www.mirrorsize.com/blogs/body-scanning-technology
4. 3DMeasureUp, "From Tailors to Tech: The Evolution of Measuring the Human Body".https://3dmeasureup.ai/blog/from-tailors-to-tech-the-evolution-of-measuring-the-human-body/
5. Heuritech, "10 Challenges the Fashion Industry Will Face in 2026", Heuritech,2026. https://heuritech.com/articles/fashion-industry-challenges/
6. Sustainability Directory, "Algorithmic Bias in Fashion Recommendation Systems", Prism Scenario. https://prism.sustainability-directory.com/scenario/algorithmic-bias-in-fashion-recommendation-systems/
7. "Incorporating Mobile Body Measuring Technology into Garment Production", 2025. https://www.tandfonline.com/doi/full/10.1080/00405000.2025.2466861?af=R
8. Center for Digital Health (Brown University), "Privacy Data Ethics of Wearable Digital Health Technology", Brown University CDH, 2023. https://cdh.brown.edu/news/2023-05-04/ethics-wearables
9. Sustainability Directory, "Wearable Data Ethics", Fashion Sustainability Directory. https://fashion.sustainability-directory.com/term/wearable-data-ethics/
10. Forbes Communications Council, "Cybersecurity as a Brand Differentiator: Building Consumer Trust", Forbes, 2025. https://www.forbes.com/councils/forbescommunicationscouncil/2025/02/24/cybersecurity-as-a-brand-differentiator-building-consumer-trust/
11. Sustainability Directory, "Cybersecurity in Fashion", Fashion Sustainability Directory. https://fashion.sustainability-directory.com/term/cybersecurity-in-fashion/
12. Sustainability Directory, "What Role Does Cybersecurity Play in Sustainable Fashion?", Fashion Sustainability Directory.https://fashion.sustainability-directory.com/question/what-role-does-cybersecurity-play-in-sustainable-fashion/
13. Sustainability Directory, "Why Is Data Privacy Important in the Fashion Industry?", Fashion Sustainability Directory.https://fashion.sustainability-directory.com/question/why-is-data-privacy-important-in-fashion-industry/
14. MD-Journal, "Ethical and Safety Considerations for Using Digital Health Technology", Medicine (MD-Journal), 2024. https://journals.lww.com/md-journal/fulltext/2024/08160/with_advancement_in_health_technology_comes_great.44.aspx
15. Digital Age Lawyers, "Privacy and Biometric Data: Legal Concerns with Wearable Sports Tech", DigitalAgeLawyers. https://digitalagelawyers.com/privacy-and-biometric-data-legal-concerns-with-wearable-sports-tech/
16. Frontiers Digital Health, "Privacy, Ethics, Transparency, and Accountability in AI Systems for Wearable Devices", Frontiers Digital Health, 2025. https://www.frontiersin.org/journals/digital-health/articles/10.3389/fdgth.2025.1431246/full

17. MDPI, "'Whispers from the Wrist': Wearable Health Monitoring Devices, MDPI Journal. https://www.mdpi.com/2410-387X/8/2/26
18. Missouri Bar News, "Every Breath You Take: Data Privacy and Your Wearable Fitness Device", MoBar News. https://news.mobar.org/every-breath-you-take-data-privacy-and-your-wearable-fitness-device/
19. Sustainability Directory, "What Are the Ethical Implications of Digitalization in Fashion?", Fashion Sustainability Directory. https://fashion.sustainability-directory.com/question/what-are-the-ethical-implications-of-digitalization-in-fashion/
20. Sustainability Directory, "What Are Ethical Concerns about AI in Fashion?", Fashion Sustainability Directory. https://fashion.sustainability-directory.com/question/what-are-ethical-concerns-about-ai-in-fashion/
21. Business of Fashion, "How Fashion Businesses Can Mitigate Cyber Risk", Business of Fashion, 2022. https://www.businessoffashion.com/articles/technology/the-state-of-fashion-2022-bof-mckinsey-cyber-security-risk-strategy/
22. Fashion Roundtable, "The Ethics of Digital Humans within Fashion Modelling (and Beyond)", Fashion Roundtable, 2024. https://www.fashionroundtable.co.uk/news/2024/7/22/the-ethics-of-digital-humans-within-fashion-modelling-and-beyond
23. Audaces, "Digital Tailor: How It Can Transform Your Apparel Manufacturing", Audaces Blog. https://audaces.com/en/blog/digital-tailor
24. CIO&Leader, "Fashion and Cybersecurity: The Intersection of Technology and the Fashion Industry", CIO&Leader. https://www.cioandleader.com/fashion-and-cyber-security-the-intersection-of-technology-and-the-fashion-industry/
25. Sustainability Directory, "What Are the Ethical Issues in Digital Fashion?", Fashion Sustainability Directory. https://fashion.sustainability-directory.com/question/what-are-the-ethical-issues-in-digital-fashion/