Joint CSCE Construction Specialty & CRC Conference 2025
Conférence conjointe spécialisée en construction de la SCGC et CRC-2025

Montreal, Quebec
July 28-31, 2025 / *28-31 juillet 2025*

PRIVACY POLICIES OF WEARABLE DEVICES FOR WORKER SAFETY AND HEALTH MONITORING IN CONSTRUCTION

Chinedu Okonkwo[1], Amanda Betancourt[1], Ibukun Awolusi[1]*, and Oluwafemi Akanfe[2]

[1] School of Civil & Environmental Engineering, and Construction Management, The University of Texas at San Antonio, San Antonio, TX, United States
[2] Department of Management, Information Systems, & Quantitative Methods, The University of Alabama at Birmingham, Birmingham, AL, United States

ABSTRACT: With the growing awareness of wearable devices' potential for enhancing construction safety and health monitoring, concerns regarding the privacy and security of collected health data have emerged as significant factors influencing adoption. The lack of industry-specific regulations on wearable technology has led construction companies to rely on off-the-shelf devices, potentially exposing them to non-compliance penalties under data protection laws such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA). To facilitate informed decision-making, this study evaluates the data privacy policies of 12 commercially available wearable devices that can be used for construction safety and health monitoring. By leveraging web scraping techniques and natural language processing, the analysis assesses the level of compliance of these devices with data privacy regulations. Five key criteria are considered: transparency in data collection, user rights in managing consent, data retention and deletion policies, data sharing with third parties, and security measures implemented. The findings are expected to inform stakeholders and policymakers in the construction sector regarding the privacy implications associated with the adoption of commercially available wearable devices. By offering insights into the privacy considerations integrated into the design and implementation of wearable devices, this research contributes to ongoing efforts to ensure the ethical use of technology in construction safety monitoring. The outcomes of this study can guide decision-making processes and support the development of policies that prioritize privacy protection while harnessing the benefits of wearable technology for improved safety in construction environments.

1. INTRODUCTION

Ensuring the safety of construction workers remains a critical concern within the industry due to the inherently hazardous nature of construction activities. Recent advancements in wearable technology have introduced innovative solutions to mitigate these risks by enabling continuous monitoring of workers' physiological conditions, environmental factors, and movement patterns (Ahn et al. 2019; Awolusi et al. 2018). Devices such as smart helmets, biometric wristbands, GPS-enabled vests, and exoskeletons facilitate real-time data collection, enhancing safety management and enabling proactive intervention strategies. These technologies contribute significantly to reducing workplace injuries by identifying potential hazards before they escalate into serious incidents.

The integration of wearable devices into construction safety and health monitoring presents substantial advantages, such as improved hazard detection, enhanced worker well-being, and increased efficiency in

responding to workplace incidents. However, as these devices become more prevalent, concerns surrounding data privacy, security, and regulatory compliance have grown (Ghafoori et al. 2023; Awolusi et al. 2024: Okonkwo et al. 2025). Wearable devices collect, store, and transmit sensitive personal information, including health metrics and real-time location data. While this data is needed for safety monitoring, it raises significant ethical and legal challenges related to data protection and user consent. Unlike industries such as healthcare, where stringent regulations govern data privacy, the construction sector lacks clear, industry-specific guidelines to regulate the use of wearable technology. As a result, construction firms frequently adopt commercially available wearable devices, potentially exposing themselves to legal risks associated with non-compliance with data protection laws such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) (Tikkinen-Piri et al. 2018).

To address these concerns and support informed decision-making, this study evaluates the privacy policies of commercially available wearable devices commonly used in construction safety monitoring. The analysis focuses on key aspects of data regulation, including data collection, storage, processing, and sharing practices with third parties. Additionally, the study examines the security measures implemented by device manufacturers, the transparency of data processing methods, and the level of compliance with established data privacy regulations. The study aims to shed light on the data security measures implemented by device manufacturers, the transparency of data processing methods, and the level of compliance of these wearables with data privacy regulations.

2. RESEARCH METHOD

A quantitative analysis comprising two main components was conducted to assess the compliance of the commercially available wearable devices included in this study. First, a compliance evaluation metric was developed to systematically assess and score the compliance levels of the privacy policies of off-the-shelf wearable devices. Second, a word frequency analysis of these privacy policies was conducted to corroborate the results of the compliance scoring process, thereby enhancing the objectivity and reliability of the analysis.

2.1 Data Collection

The data collection process involves the search and identification of popular off-the-shelf WIoT devices used in construction. The search for off-the-shelf WIoT devices relied on data that the manufacturers or vendors made publicly available for the devices. The "Google" search engine was used, and keywords derived from the identified applications of WIoT devices for safety and health monitoring in construction were adopted. The privacy policies of these identified devices were extracted manually and compiled for analysis. These applications include physiological monitoring, environmental sensing, and proximity and location tracking (Okonkwo et al. 2025). The privacy policies of the devices were collected and stored. Only wearable devices with available privacy policies and commercially available for purchase are included in this study. The devices identified based on the search and included in this study are Kenzen, Blackline Safety's G7c, Spot-r, CORE sensor GreenTEG, Apple watch series, Galaxy watch, Hexoskin Smart garments, Smart helmet + Smart band, Fitbit sense, Empatica, Slatesafety Band V2, and SoterCoach.

2.2 Privacy Compliance Evaluation

The collected privacy policies were evaluated or analyzed for compliance with the regulations of GDPR (General Data Protection Regulation) and HIPAA (Health Insurance Portability and Accountability Act). The policies were evaluated based on the following criteria identified from the review of existing studies (Agarwal et al. 2018; Bakare et al. 2024; Labadie and Legner, 2023; Okonkwo et al. 2025):

- **Transparency**: What types of data (physiological, location, environmental) are collected by the wearable devices, and how is this information described in the privacy policies?
- **User Rights**: How does the policy describe user consent? Does it allow users to opt in and out of data collection, and are there clear methods for obtaining consent?

- **Data Retention and Deletion**: How long is data retained, and under what conditions is it deleted? This includes whether the policies provide specific retention periods or leave the timeline vague.
- **Data Sharing and Third Parties**: How are the data-sharing practices described? Do the devices share data with third parties, and is it clear who these third parties are and how they will use the data?
- **Data Security Measures**: What types of security measures are described (e.g., encryption, access controls) to protect the data collected and processed by these devices?

Each criterion was assigned a score from 1 - 5, and an overall compliance score was calculated for each device. The compliance scores are used to rank the level of compliance of each device to data privacy and security standards. Table 1 provides a full description of the privacy compliance metric used to assess the policies' compliance based on the five criteria above.

Table 1: Privacy Compliance Evaluation Scoring Metric

Score	Criteria
Transparency	
1	**Very Low Transparency**: The policy provides little to no information about the types of data collected or the purpose of collection.
2	**Low Transparency**: The policy mentions data collection but is vague about the types collected and their specific purposes.
3	**Moderate Transparency**: The policy specifies some types of data collected (e.g., "location data," “health data”) but lacks detail about all types collected or their purposes.
4	**High Transparency**: The policy clearly identifies most types of data collected and provides a general explanation for why each type is collected.
5	**Full Transparency**: The policy explicitly lists all types of data collected and provides a specific, detailed purpose for each type.
User Rights	
1	**Very Limited User Control**: The policy barely mentions user consent, lacks opt-in/out options, and does not describe methods for obtaining consent.
2	**Low User Control**: Mentions consent but is vague on how it is obtained.
3	**Moderate User Control**: The policy provides basic consent details and includes opt-out options.
4	**High User Control**: The policy clearly explains how consent is obtained and includes explicit opt-in and opt-out options, but it may lack detailed instructions for managing consent.
5	**Full User Control**: The policy provides a comprehensive description of how consent is obtained and includes clear opt-in and opt-out options.
Data Retention and Deletion	
1	**Very Limited Information**: The policy does not mention data retention timelines or deletion practices.
2	**Low Detail**: Mentions data retention but provides little or no specifics on how long data is retained or conditions for deletion.
3	**Moderate Detail**: Specifies some data retention periods and provides general information on deletion practices
4	**High Detail**: The policy provides clear retention timelines for most data types and explains conditions under which data will be deleted, but it may lack details for certain data types
5	**Full Detail**: The policy explicitly states retention periods for all data types, outlines specific conditions for data deletion, and provides a clear explanation of retention and deletion practices.
Data Sharing and Third Party	
1	**No Disclosure**: The policy does not mention data-sharing practices or any third-party involvement.
2	**Minimal Disclosure**: Mentions data sharing vaguely but does not specify who the third parties are or how they will use the data.
3	**Moderate Disclosure**: The policy identifies some third parties and provides basic information on why data is shared but lacks detail on all third-party relationships
4	**High Disclosure**: The policy clearly identifies most third parties and provides specific purposes for sharing data, but may lack details for some minor data-sharing arrangements.

5	**Full Disclosure**: The policy comprehensively details all third parties involved, explicitly states the purpose of each data-sharing relationship, and explains how each party will use or protect the data.
Data Security Measures	
1	**No Mention of Security**: The policy does not reference any data security measures or protections.
2	**Minimal Security Information**: Mentions general security practices but does not specify types of security measures.
3	**Basic Security Measures**: Mentions at least one security measure but lacks detail on implementation or comprehensive coverage across all data types.
4	**High Level of Security Detail**: Provides a clear description of multiple security measures, but may lack detail on specific conditions or advanced measures like regular security audits.
5	**Comprehensive Security Information**: The policy provides detailed information on a full range of security measures for protecting all data types.

To minimize bias and subjectivity in ranking privacy policies, three experts with backgrounds and expertise in construction, wearable technology, information systems, privacy policy, and regulatory compliance were selected. These experts possess advanced degrees at the master's and doctoral levels with industry and research experience ranging from 10 to 15 years. Each expert independently evaluated and scored the privacy policies, a process that helped eliminate potential influence from group dynamics or consensus-driven behaviors. Interrater agreement was assessed by analyzing any disparities in their rankings to ensure consistency. Where significant differences in scoring emerged, the experts engaged in discussions to clarify interpretations and resolve inconsistencies. The inter-rater agreement is calculated using Fleiss' Kappa formula shown below.

$$k = \frac{Po - Pe}{1 - Pe} \quad (1.0)$$

Where P_o is the observed agreement, and P_e is the expected agreement by chance.

2.3 Word Frequency Analysis

Word frequency analysis was conducted to identify dominant privacy-related expressions within the policies and evaluate whether these high-frequency terms align with the key regulatory principles outlined in the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA). Specifically, we aimed to assess the extent to which the language used by wearable device manufacturers reflects the core tenets of GDPR and HIPAA. The Natural Language Toolkit (NLTK) was adopted for word frequency analysis. NLTK is a versatile Python library for processing and analyzing human language data (Batta 2024). It offers a wide range of functionalities, including tokenization, stemming, and parsing, making it valuable for various natural language processing tasks (Farkiya et al. 2015). Natural Language Toolkit (NLTK) has been widely applied for word frequency analysis in various research contexts. Kumar and Rani (2021) employed NLTK's word frequency algorithms for paragraph summarization, extracting key points from lengthy texts. In corpus research, Wang and Hu (2021) demonstrated NLTK's flexibility and rich functionality for text cleaning, word form restoration, part-of-speech tagging, and text retrieval statistics, using US presidential inaugural speeches as an example. These studies collectively demonstrate NLTK's versatility and effectiveness in word frequency analysis across diverse domains. The dataset used for this analysis included twelve full privacy policies of the 12 identified devices. These data were collected manually from official product websites and saved in plain text format. In total, the combined dataset comprised 25,077 words.

A text preprocessing process in which the privacy policies were first preprocessed using standard NLP techniques was conducted. This process includes:

- **Tokenization**: Breaking down the text into individual words or phrases.
- **Stop Word Removal**: Removing common words (e.g., "and," "the") that do not add meaning to the analysis.
- **Lemmatization/Stemming**: Reducing words to their base form to ensure consistent analysis (e.g., "collecting" becomes "collect").

3. RESULTS AND DISCUSSION

3.1 Summary of Privacy Policy of the Wearable Devices

Table 2 below summarizes key privacy and data protection attributes for various wearable devices commonly used in construction. It outlines the types of data each device collects (such as physiological, environmental, and location data) and how user consent is managed, including any mechanisms for opting in or out of data collection. The Table also specifies the data retention and deletion policies, indicating how long user data is stored and under what conditions it may be deleted. Additionally, it includes information on data-sharing practices, listing third-party involvement, and any legal or business-related sharing requirements. Finally, the Table describes the security measures for each device, such as encryption, access controls, and administrative protections, which are essential for safeguarding user privacy and data integrity in high-risk environments like construction. Given that most wearable devices are designed for individual use, the term “End-User” or “User” in the included policies often refers to the individual whose personal data (physiological metrics, location, and environmental exposure) is being collected, processed, and potentially shared. while the organizational buyer can be considered the legal “end-user” of the device platform, the focus of this study is not on legal ownership of devices, but on the privacy risks and protections afforded to individual workers based on the publicly disclosed practices within these policies.

Table 2: Privacy Policy Attributes of Wearable Devices

Wearable Device	Privacy Policy Attributes				
	Data Collection	User Consent Mechanism	Data Retention and Deletion	Data Sharing	Security Measures
Kenzen	Physiological, Environmental, and location	Users can withdraw or limit consent anytime (EULA)	Not specified	Shared with third parties for legal/business use	Administrative, contractual, physical, and technical protections
Blackline Safety’s G7c	Environmental and location	Withdraw or limit consent anytime (EULA)	Deleted 3 post-termination	Shared with third parties for legal/business use	Not specified
Spot-r	Physiological and location	EULA	Not specified	Shared with third parties for legal/business use	Not specified
CORE sensor GreenTEG	Physiological, Environmental, and location	Consent obtained at multiple points; user-controlled	Deletable upon user request	Shared with third parties for legal/business use	Administrative, organizational, and technical
Apple watch series 6	Physiological and location	Withdraw or limit consent anytime (EULA)	Not specified	Shared with third parties for legal/business use	Administrative, physical, and technical
Galaxy watch 3	Physiological and location	Withdraw or limit consent anytime (EULA)	Not specified	Shared with third parties for legal/business use	physical and technical
Hexoskin Smart garments	Physiological	Withdraw consent anytime (EULA)	Deleted upon service termination	Shared with third parties for legal/business use	firewalls, encryption, and authentication
Smart helmet + Smart band	Physiological	Withdraw or limit consent anytime (EULA)	Not specified	Shared with third parties for legal/business use	Organizational protections
SoterCoach	Physiological	Withdraw or limit consent anytime (EULA)	Deleted after 5 years or by request	Shared with third parties for legal/business use	Organizational and technical protections
Empatica	Physiological and location	Withdraw or limit consent anytime (EULA)	Deleted after 10 years or by request	Shared with third parties for legal/business use	Administrative physical, personnel, and technical
Fitbit Sense	Physiological and location	Withdraw or limit consent anytime (EULA)	Not specified	Shared with third parties for legal/business use	Administrative physical, and technical

EULA: End-user license agreement

To evaluate GDPR compliance, this study assessed wearable device policies against key articles. Article 5, which outlines principles like data minimization and purpose limitation (intersoft consulting 2025), was fully addressed by only a few devices such as Empatica and CORE Sensor, while nearly 60% used vague terms such as “personal data” without clear justification for collection. Article 6 requires lawful processing, typically user consent, but only four devices offered explicit opt-in/opt-out mechanisms; others relied on implied consent through device usage. Article 15, which ensures data subject access rights, was rarely supported, with fewer than 25% of devices allowing users to view or manage their data. Although most manufacturers are not HIPAA-covered entities, their processing of health-related data suggests a need to meet similar expectations under the Privacy and Security Rules, which were only partially addressed in a minority of policies.

3.2 Word Frequency Analysis of the Wearable Devices

The word frequency analysis of the privacy policies of all the wearable devices included in this study, depicted in Figure 1, reveals key areas of focus that reflect the primary concerns and operational practices of these devices.

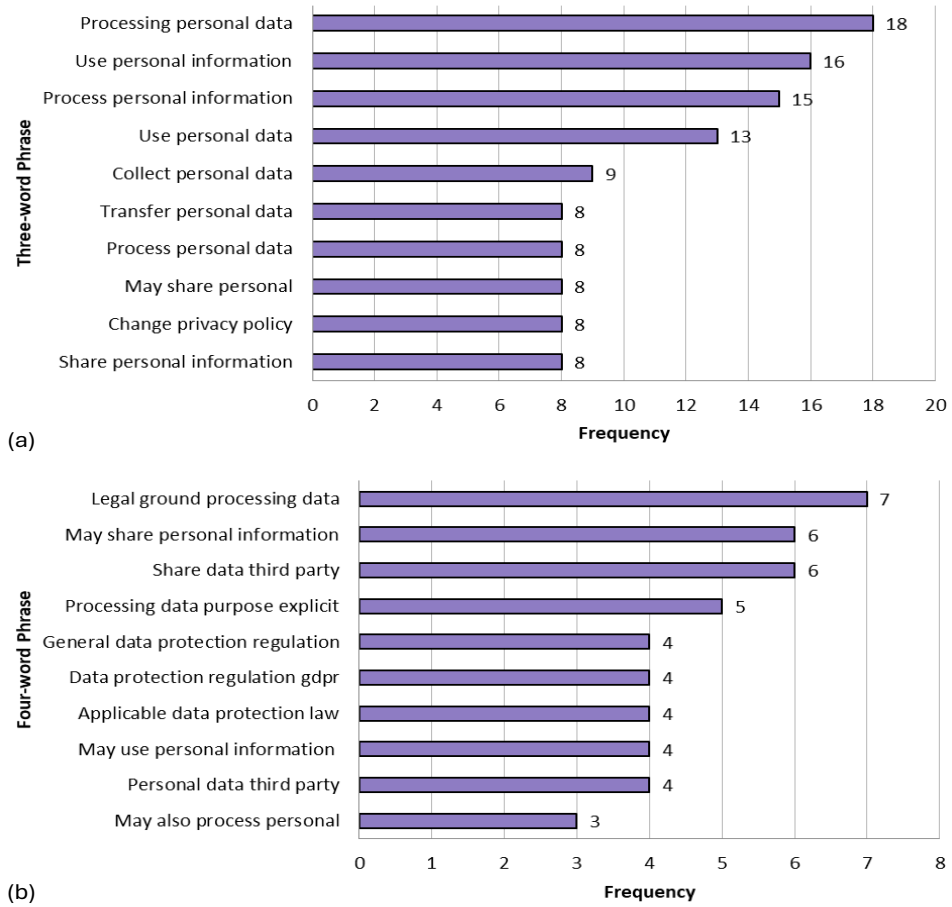

Figure 1: (a) Three-word and (b) Four-word Frequency Analysis of Privacy Policies of WIoT

The high frequency of phrases like "Processing personal data," "Use personal information," and "Process personal information" in the three-word chart highlights a significant emphasis on the handling and usage of user data. This suggests that wearable device policies are keen to communicate how personal information is managed, processed, and utilized, likely in response to regulatory demands and user expectations around data transparency and responsible usage. Wearable devices collect extensive personal data for health monitoring, fitness tracking, and location services, making it critical for policies to specify how this data is processed to ensure compliance and build user trust. Additionally, phrases such as

"Collect personal data" and "Transfer personal data" indicate a focus on data collection and movement, emphasizing that wearable devices gather sensitive information, which may be transferred across different platforms or third-party services. This is further evidenced by the four-word frequency chart, where "Share data third party" and "May share personal information" are prominent. These phrases suggest that sharing user data with third parties, possibly for analytics, service enhancement, or compliance purposes, is a common practice in wearable device operations. This emphasis on data sharing reflects an industry standard where third-party collaborations are necessary yet also calls for transparency to mitigate user privacy concerns.

Moreover, the frequent appearance of "Legal ground processing data" and "General data protection regulation" in the four-word chart demonstrates that wearable device policies heavily reference legal justifications and compliance with data protection regulations like GDPR. This focus indicates that wearable devices are intended to align with legal standards, particularly around data processing rights, lawful bases for data usage, and explicit explanations of data handling practices. This attention to regulatory language not only aims to fulfill legal obligations but also seeks to enhance the credibility of wearable devices in handling personal data responsibly.

3.3 Compliance Level Scoring of the Wearable Devices

Table 3 presents the average privacy compliance scores assigned by three expert raters to various wearable devices, with a robust interrater agreement reflected by a Kappa value of 0.86, indicating strong consistency among raters. Each device is evaluated across five criteria: transparency, user rights, data retention and deletion, data sharing with third parties, and data security measures. Scores range from 1 to 5 for each criterion, with higher scores indicating stronger compliance. The Table also includes a total score and a compliance percentage for each device, which gives an overall view of how well each device aligns with privacy standards, such as GDPR and HIPAA, highlighting areas where certain devices excel or fall short in privacy and data protection.

Table 3: Privacy Compliance Scoring Result for the Wearable Devices

Policy	Transparency	User Rights	Data Retention and Deletion	Data Sharing and Third Party	Data Security Measures	Total	Compliance Level
Apple Watch	3	3	3	4	3	16	64%
Blackline Safety's G7c	5	4	5	3	2	19	76%
Empatica	5	5	5	4	4	23	92%
Fitbit	5	4	3	4	4	20	80%
CORE Sensor GreenTEG	5	5	3	4	4	21	84%
Galaxy watch	3	3	3	4	3	16	64%
Hexoskin Smart Garments	5	2	1	1	4	13	52%
Kenzen	5	4	2	3	4	18	72%
Slatesafety	5	5	1	5	3	19	76%
Smart Helmet + Smart Band	3	5	3	3	2	16	64%
SoterCoach	5	3	5	4	3	20	80%
Spot-r	4	2	1	2	2	11	44%

3.3.1 Transparency

In the construction industry, transparency in data collection is not only a regulatory requirement but also crucial for building trust among workers who may already feel apprehensive about wearable devices tracking their personal data. For instance, devices like the Empatica, which scored high on transparency by clearly detailing the types of data collected and their intended uses, could be better accepted by workers on sites where high-risk activities, like working at heights or with heavy machinery, require constant monitoring of heart rate and location. Conversely, devices with moderate transparency, such as the Galaxy Watch, may create unease among workers due to their ambiguous policies. This ambiguity can lead to mistrust, affecting the overall acceptance of WIoT on sites. For example, in large construction projects, unions or worker advocacy groups could demand more comprehensive disclosure about what data is collected and for what purpose. Practical implications could include workshops or onboarding sessions where device capabilities and data practices are clearly explained to workers, thereby fostering transparency and mitigating concerns.

3.3.2 User Rights

Devices like CORE Sensor GreenTEG and Empatica, which scored high in user rights, offer significant benefits in terms of worker autonomy, allowing employees to manage their consent and withdraw it when desired. In the high-stress environment of construction, where health metrics may be collected continuously, these features reassure workers that they retain control over their personal information, unlike devices with limited user rights, such as Hexoskin and Spot-r, that risk alienating workers who feel that they have insufficient control over their data. This could lead to compliance issues, as disgruntled workers may refuse to wear such devices, defeating the purpose of implementing WIoT for safety monitoring.

3.3.3 Data Retention and Deletion

Retention policies have direct implications for construction companies in managing data storage costs, minimizing legal liability, and ensuring compliance with data privacy regulations. For instance, Blackline Safety G7c's clear retention guidelines—where data is deleted 3 years post-contract termination or upon user request—reduce the risks associated with indefinite data storage, such as breaches or misuse. This is especially important in construction, where transient workers or subcontractors are common, and data may accumulate over time. In practical application, devices without clear retention timelines, like Spot-r, pose significant risks. If data from a high-profile project is held indefinitely, it could become a liability if there is a future data breach or if workers seek to exercise their "right to be forgotten." Construction firms, particularly those handling sensitive projects (e.g., government buildings), should prioritize devices with well-defined retention policies to mitigate the risks of data-related litigation. Implementing device-specific policies for data deletion upon project completion or employment termination is an effective step toward addressing these concerns practically.

3.3.4 Data Retention and Deletion

Construction projects often involve multiple stakeholders, including contractors, clients, and regulatory bodies, which complicates data sharing. Devices like Fitbit and CORE Sensor GreenTEG, which specify their third-party sharing policies, are better suited to such environments, as these devices enable clearer communication about where data goes and why. For example, on a high-security project, knowing which entities have access to worker health data is crucial, as unauthorized sharing could jeopardize project security. Devices with vague data-sharing policies could expose construction firms to reputational damage if sensitive worker data is inadvertently shared with unauthorized parties. Practical steps to mitigate these issues include selecting WIoT devices with transparent third-party policies and establishing clear data-sharing agreements with contractors and third-party service providers. Firms can also create data-sharing "white lists" and ensure that only essential data is shared for project needs, limiting unnecessary exposure.

3.3.5 Data Security Measures

Different stakeholders are typically engaged in a construction project, such as contractors and clients, and data security is paramount where breaches could compromise not only worker privacy but also operational safety. Empatica and SoterCoach, which scored highly in security measures by detailing encryption and access control, are ideal for environments where sensitive data is gathered, such as confined spaces or remote locations. For instance, in tunnel construction, where environmental monitoring is crucial, high-security WIoT devices can monitor toxic gas levels and worker vitals without the risk of data leaks. However, devices that lack comprehensive security disclosures pose challenges in high-risk construction scenarios where data breaches could compromise both worker safety and project integrity. Construction companies should implement strict data protection protocols, using devices with clear security measures and supplementing them with additional security layers, such as periodic security audits and breach notification systems.

The aggregated compliance scores reveal a notable range in adherence to privacy standards. High-performing devices like Empatica (92%) and CORE Sensor GreenTEG (84%) demonstrate a commendable commitment to privacy, with well-defined policies that align with GDPR and HIPAA standards. This analysis underscores the importance of stringent privacy practices for WIoT devices in construction safety. High-compliance devices demonstrate that with careful policy structuring, even commercially available wearables can meet regulatory standards and safeguard worker data. However, the variability in compliance scores calls for industry-wide standards and possibly regulation to guide manufacturers in creating privacy-centric policies, ensuring all WIoT devices in construction offer robust data protection aligned with legal frameworks. The adoption of such standards will promote greater trust and acceptance of wearable technologies in high-risk industries.

4. CONCLUSIONS

The privacy compliance level of commercially available wearable devices to existing regulations was assessed in this study. The findings revealed gaps in the privacy policies, raising concerns about data security, regulatory compliance, and user autonomy. The analysis identified considerable variability in compliance levels, with a range of 44% to 92% compliance level and an average compliance level of about 70% for the 12 devices. The low-compliant devices lacked transparency in data handling, offering limited user control over consent and failing to specify data retention and deletion policies. These discrepancies highlight the need for standardized privacy regulations tailored to wearable technology in construction. A key concern is the lack of explicit data retention and deletion policies in many devices, with about 75% of the devices not specifying a retention timeline for collected data, thus raising concerns about indefinite data storage and potential misuse. Additionally, data-sharing practices remain unclear, with many devices failing to outline third-party data recipients and purposes clearly. Only a few devices provide clear guidelines on third-party data sharing, ensuring user control over their information. This study highlights that while wearable devices have the potential to improve construction safety, their effectiveness must not come at the cost of worker privacy and security**.** Future research can improve existing privacy frameworks for adopting wearable devices for safety monitoring to make them more robust for easy implementation.

While this study provides valuable insights into the privacy practices of wearable devices used in construction safety monitoring, it is not without limitations. One key limitation is the relatively small pool of expert raters (n=3) used in evaluating the privacy policies, which may affect the generalizability of the compliance scoring despite the high interrater agreement achieved. Furthermore, the analysis was based solely on publicly available privacy policy documents, which may not reflect the full spectrum of internal data handling practices employed by device manufacturers. The scope was also limited to 12 commercially available devices, potentially overlooking niche or emerging solutions with different privacy frameworks. Future research should involve a larger and more interdisciplinary panel of experts, including legal scholars, and industry practitioners, to enhance the robustness of policy evaluations. Additionally, incorporating stakeholder interviews, such as with construction managers, workers, and vendors, can provide a more contextualized understanding of policy implementation in real-world settings. Longitudinal studies are also recommended to track changes in privacy policies over time, especially in response to evolving regulations like GDPR, HIPAA, and emerging AI governance frameworks.

ACKNOWLEDGMENTS

This research was funded in part by The University of Texas at San Antonio, Office of the Vice President for Research, Economic Development, and Knowledge Enterprise through the Internal Research Awards (INTRA) program.

REFERENCES

Agarwal, S., Steyskal, S., Antunovic, F., and Kirrane, S. 2018. Legislative Compliance Assessment: Framework, Model and GDPR Instantiation. In M. Medina, A. Mitrakas, K. Rannenberg, E. Schweighofer, and N. Tsouroulas (Eds.), *Privacy Technologies and Policy* (pp. 131–149). Springer International Publishing. https://doi.org/10.1007/978-3-030-02547-2_8

Ahn, C. R., Lee, S., Sun, C., Jebelli, H., Yang, K., and Choi, B. 2019. Wearable Sensing Technology Applications in Construction Safety and Health. *Journal of Construction Engineering and Management*, *145*(11), 03119007. https://doi.org/10.1061/(ASCE)CO.1943-7862.0001708

Awolusi, I., Marks, E., and Hallowell, M. 2018. Wearable technology for personalized construction safety monitoring and trending: Review of applicable devices. *Automation in Construction*, *85*, 96–106. https://doi.org/10.1016/j.autcon.2017.10.010

Awolusi, I., Nnaji, C., Okpala, I., and Albert, A. 2024. Adaptation behavior of construction workers using wearable sensing devices for safety and health monitoring. *Journal of Management in Engineering*, *40*(1), 04023055.

Bakare, S. S., Adeniyi, A. O., Akpuokwe, C. U., and Eneh, N. E. 2024. Data privacy laws and compliance: a comparative review of the EU GDPR and USA regulations. *Computer Science & IT Research Journal*, *5*(3), Article 3. https://doi.org/10.51594/csitrj.v5i3.859

Barrett, N., and Weber-Jahnke, J. H. 2009. Applying Natural Language Processing Toolkits to Electronic Health Records – An Experience Report. In *Advances in Information Technology and Communication in Health* (pp. 441–446). IOS Press. https://doi.org/10.3233/978-1-58603-979-0-441

Farkiya, A., Saini, P., and Sinha, S. 2015. *Natural Language Processing using NLTK and WordNet*. https://www.semanticscholar.org/paper/Natural-Language-Processing-using-NLTK-and-WordNet-Farkiya-Saini/0414c4cc1974e6d3e69d9f2986e5bb9fb1af4701

Ghafoori, M., Clevenger, C., Abdallah, M., and Rens, K. 2023. Heart rate modeling and prediction of construction workers based on physical activity using deep learning. *Automation in Construction*, *155*, 105077. https://doi.org/10.1016/j.autcon.2023.105077

intersoft consulting. 2025. *Principles relating to processing of personal data*. General Data Protection Regulation (GDPR). Retrieved April 10, 2025, from https://gdpr-info.eu/chapter-1/

Kumar, G. K., and Rani, D. M. 2021. *Paragraph summarization based on word frequency using NLP techniques*. 060001. https://doi.org/10.1063/5.0037283

Labadie, C., and Legner, C. 2023. Building data management capabilities to address data protection regulations: Learnings from EU-GDPR. *Journal of Information Technology*, *38*(1), 16–44. https://doi.org/10.1177/02683962221141456

Okonkwo, C., Awolusi, I., Nnaji, C., and Akanfe, O. 2025. Privacy and security of wearable internet of things: A scoping review and conceptual framework development for safety and health management in construction. *Computers & Security*, *150*, 104275. https://doi.org/10.1016/j.cose.2024.104275

Tikkinen-Piri, C., Rohunen, A., and Markkula, J. 2018. EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, *34*(1), 134–153. https://doi.org/10.1016/j.clsr.2017.05.015

Venkata Mahesh Babu Batta. 2024. Human Language Data Processing using NLTK. *International Journal of Advanced Research in Science, Communication and Technology*, 628–634. https://doi.org/10.48175/IJARSCT-17685

Wang, M., and Hu, F. 2021. The Application of NLTK Library for Python Natural Language Processing in Corpus Research. *Theory and Practice in Language Studies*, *11*(9), 1041–1049. https://doi.org/10.17507/tpls.1109.09