Received 27 September 2025
Revised 5 May 2026
8 July 2026
Accepted 10 July 2026

Workplace adoption of wearable devices: insights into Greek employees' intentions and usage trends

Maria Vasilidou, Anastasios Diamantidis, Despoina Ioakeimidou, Ioannis Kansizoglou, Symeon Symeonidis, Prodromos Chatzoglou and Antonios Gasteratos
Production and Management Engineering, School of Engineering, Democritus University of Thrace, Xanthi, Greece

Abstract

Purpose – This study aims to investigate the factors influencing Greek employees' intention to adopt wearable devices in the workplace, focusing on privacy management and trust. It addresses the organizational challenges of balancing innovation with employee concerns about surveillance and data protection.

Design/methodology/approach – Based on Privacy Calculus Theory, extended with trust, a research model was tested through a large-scale survey of 2,243 employees in Greece using structural equation modeling.

Findings – Perceived effectiveness of privacy policies, control and benefits strongly predicted adoption intention, while privacy concerns and risks acted as barriers. Trust showed limited direct effects, with its influence primarily operating through indirect relationships. The model explained 46% of adoption intention variance.

Practical implications – The findings highlight the importance for managers to design transparent privacy policies, strengthen employee control over data and build organizational trust to facilitate wearable integration into HR and productivity practices.

Originality/value – The study extends Privacy Calculus Theory to organizations, introduces institutional variables such as privacy policy effectiveness and clarifies trust's indirect role. It provides new insights from a regional context rarely examined.

Keywords Wearable devices, Privacy calculus theory, Employee intention, Organizational technology acceptance

Paper type Research paper

1. Introduction

The rapid advancement of digital technologies has transformed workplaces, with wearables emerging as a fast-growing trend valued at nearly $70bn in 2019 (Shen *et al.*, 2022). These internet-connected devices (e.g. smartwatches, VR and EEG headsets, fitness trackers) collect and transmit physical, cognitive or emotional data (Sun and Gu, 2024; Singh, 2023;

Funding: This study was conducted within the framework of the project "Greece 4.0: Network of excellence for Development, Dissemination & Implementation of Digital Transformation Technologies in Greek Manufacturing Industry" (TAEDR-0535864), funded by the National Recovery and Resilience Plan Greece 2.0, financed by the European Union – NextGenerationEU.

Journal of Science and Technology Policy Management
Vol. 17 No. 11, 2026
pp. 100-122
Emerald Publishing Limited
2053-4620
DOI 10.1108/JSTPM-09-2025-0450

Rahman *et al.*, 2022; Felea *et al.*, 2021; Sergueeva *et al.*, 2020; Shafique *et al.*, 2019; Debnath *et al.*, 2018; Canhoto and Arp, 2017; Khakurel *et al.*, 2017; Wright and Keith, 2014). In organizational contexts, they are promoted for monitoring productivity, enhancing safety and supporting employee well-being (Jacobs *et al.*, 2019).

Despite these potential benefits, the organizational adoption of wearable technologies remains limited due to concerns regarding data protection and trust in employers. Although research on wearable technology adoption has grown considerably, most existing studies have focused on consumer contexts rather than organizational settings (Al-Emran *et al.*, 2023; Kim and Chiu, 2019; Canhoto and Arp, 2017; Chuah *et al.*, 2016; Jung *et al.*, 2016; Lee *et al.*, 2016; Lunney *et al.*, 2016; Yang *et al.*, 2016; Kim and Shin, 2015; Zhang and Rau, 2015). Employees often perceive wearables not only as tools for efficiency but also as instruments of surveillance. These contrasting perceptions make it important to examine not only employees' willingness to adopt wearable technologies but also the organizational conditions and governance mechanisms under which such adoption becomes acceptable (Fox *et al.*, 2021; Magni *et al.*, 2021; Yun *et al.*, 2019; Wirth, 2018; Xu *et al.*, 2011).

In this context, the organizational environment differs fundamentally from consumer settings, as employees' decisions are shaped by hierarchical relationships, limited autonomy and the potential use of data for monitoring and performance evaluation. These conditions suggest that privacy-related perceptions, control and trust may operate differently in workplace environments, extending the application of Privacy Calculus Theory.

To achieve effective integration of wearable technologies, organizations must balance data collection with privacy protection (Fox *et al.*, 2021; Jozani *et al.*, 2020). Previous studies also suggest extending research beyond smartwatches and adopting theoretical frameworks other than the technology acceptance model (TAM), which primarily emphasizes ease of use and usefulness (Shafique *et al.*, 2019; Asadi *et al.*, 2019; Lin *et al.*, 2007; Davis, 1989). Scholars further highlight the need to incorporate trust as a determinant of adoption, given its role in shaping employee perceptions of data disclosure (Duan and Deng, 2021; Kim and Chiu, 2019).

Moreover, prior research is geographically concentrated in countries such as the USA, China and Ireland, limiting generalizability, while evidence from Southern Europe and developing economies remains scarce (Liang *et al.*, 2024; Duan and Deng, 2021; Rowe, 2020; Asadi *et al.*, 2019; Li *et al.*, 2016; Gao *et al.*, 2015). The present study aims to address these gaps by examining the factors that influence employees' intention to adopt wearable devices in the workplace. Grounded in Privacy Calculus Theory and extended with trust, it explores how perceptions of privacy policies, control, risks and benefits shape adoption. The research focuses on Greece, a country where organizational adoption of wearables is still at an early stage and official statistics cover mainly internet and computer use (Hellenic Statistical Authority, 2023).

Using a large and diverse sample of employees across age groups and occupational sectors, the study captures perspectives before large-scale implementation, providing insights into both opportunities and barriers to integration (Al-Emran *et al.*, 2023; Magni *et al.*, 2021; Kim and Chiu, 2019; Shafique *et al.*, 2019; Guo *et al.*, 2012; Xu *et al.*, 2011). Based on the above, the study addresses the following research question:

RQ1. What factors influence employees' intention to adopt wearable devices in the workplace, and how do privacy-related perceptions, control, risks, benefits and trust shape this decision within an organizational context?

2. Literature review

2.1 Related studies on wearable devices adoption

The adoption of, and intention to use, wearable technologies devices have been widely studied across population groups such as adolescents, elderly, parents and consumers (Rahman *et al.*, 2022; Magni *et al.*, 2021; Cilliers, 2020; Dwivedi *et al.*, 2019; Tavares and Oliveira, 2018; Khakurel *et al.*, 2018; Nalchigar and Yu, 2018; Wang *et al.*, 2018; Ng *et al.*, 2017; Lismont *et al.*, 2017; Mendoza *et al.*, 2017; Kerner and Goodyear, 2017; Rogers and Park, 2016; Lunney *et al.*, 2016; Turhan, 2013).

Most studies on wearable technology adoption have focused on health-monitoring devices (Ren *et al.*, 2023; Asadi *et al.*, 2019). Using the TAM, Felea *et al.* (2021) found, based on a sample of 192 students, that young people being receptive and curious about technology, have a natural predisposition to acceptance. Similarly, Mohammed and Redzuan (2020), based on a survey of 304 parents, concluded that wearable devices are not adopted due to privacy concerns and concerns about data security. Li *et al.* (2019) examined the acceptance of wearable health devices among older adults, while Chiu *et al*. (2018) investigated the adoption of sports and fitness wearables among Korean consumers (sample 146 and 247, respectively). Previous studies consistently identify privacy concerns, perceived privacy risks, limited organizational support and insufficient incentives for personal data disclosure as key barriers to wearable technology adoption (Singh, 2023; Tang and Ning, 2023; Xu *et al.*, 2011).

Although wearable technology adoption has been widely examined across different population groups, most existing studies focus on consumer-oriented contexts, where technology use is typically voluntary and driven by individual preferences. In contrast, research addressing employees and the organizational benefits of wearable device use remains limited. However, organizational settings introduce additional dimensions, such as hierarchical relationships, performance monitoring and data governance, which may significantly influence employees' perceptions and decision-making processes. Recent research further highlights that AI-enabled employee surveillance and digital monitoring practices may undermine workplace trust unless supported by transparent governance and ethical HRM practices (Qureshi *et al.*, 2026).

In this context, wearable technologies in the workplace cannot be examined solely through the lens of technology acceptance, as they are closely associated with broader organizational dynamics. In particular, the use of wearable devices is often linked to workplace surveillance and employee monitoring practices, raising concerns about autonomy, fairness and power asymmetries between employees and employers (Moore, 2017; Ball, 2010). Existing research highlights that data collection in organizational environments is not neutral but embedded in governance structures that define how employee data are accessed, interpreted and used (Kellogg *et al.*, 2020; Ajunwa *et al.*, 2017).

Moreover, the increasing datafication of work has intensified the importance of organizational trust and transparency, as employees must rely on their employers to manage sensitive personal data responsibly (Pawirosumarto and Kurniawan, 2026; Ball, 2010). Recent conceptual work further argues that the effects of workplace surveillance depend not only on monitoring itself but also on how HRM systems are designed, particularly regarding transparency, employee participation and organizational governance (Patel *et al.*, 2026). These issues position wearable adoption within a wider framework of organizational data governance, where privacy, control and trust are shaped not only by individual perceptions but also by institutional policies, governance mechanisms and workplace surveillance regulations (Howe *et al.*, 2026).

Magni *et al.* (2021) empirically investigated the intention to use wearable devices in an organizational environment using an expanded TAM with a sample of 523 temporary employees. Jacobs *et al.* (2019) made an important contribution by demonstrating, through a sample of 1,273 employees, the organizational conditions required for the successful implementation of wearable technology programs. Using the Theory of Planned Behavior (TPB), Shafique *et al.* (2019) conducted a case study with a sample of 150 employees in pharmaceutical companies and examined the relationship between wearable device adoption and organizational benefits.

2.2 *Privacy Calculus Theory*

Privacy Calculus Theory posits that individuals decide whether to disclose personal data by weighing the perceived benefits against the associated privacy risks (Tang and Ning, 2023; Liu *et al.*, 2021; Jozani *et al.*, 2020; Dinev and Hart, 2006). When perceived benefits outweigh perceived risks, individuals are more likely to adopt a technology, although this balance may vary across different contexts (Fox *et al.*, 2021; Li *et al.*, 2016; Gao *et al.*, 2015). The theory also encompasses related constructs, including perceived privacy control, privacy concerns and the perceived effectiveness of privacy policies.

Privacy Calculus Theory was selected as the theoretical foundation of this study because it captures both the findings of prior research and the distinctive characteristics of organizational settings. Unlike models such as TAM, which primarily emphasize perceived usefulness and ease of use, Privacy Calculus Theory focuses on the fundamental trade-off employees face when adopting workplace wearables: potential gains in productivity, safety, or personalization versus privacy loss, surveillance and reduced trust. Its adaptability across contexts involving sensitive personal data makes it particularly suitable for workplace research, where technology adoption decisions are influenced not only by individual preferences but also by organizational policies, governance mechanisms and power relationships (Fox *et al.*, 2021; Li *et al.*, 2016).

3. Research model and hypothesis development

Privacy Calculus Theory offers flexibility to evaluate technology adoption through a cost-benefit lens. It is particularly suitable for workplace wearables, where employees often have limited prior experience and must balance perceived benefits against risks. To extend prior models, this study incorporates "trust" as an additional factor shaping adoption intention (Fox *et al.*, 2021; Trepte *et al.*, 2020; Jozani *et al.*, 2020). The proposed research model is presented in Figure 1.

3.1 *Perceived effectiveness of privacy policy*

Effective corporate privacy policies inform employees how their data will be used and provide safeguards against misuse. When employees perceive such policies as credible, they are more likely to trust their employer, feel a sense of control and perceive fewer risks (Tang and Ning, 2023; Xu *et al.*, 2011; Milne and Culnan, 2004):

H1. Perceived effectiveness of privacy policy is positively associated with perceived benefits.

H2. Perceived effectiveness privacy policy is negatively associated with perceived risk.

H3. Perceived effectiveness privacy policy is positively associated with employee perception of privacy control.

3.2 *Privacy control*

Privacy control refers to employees' belief that they can decide how much data to share and how it is disseminated. Higher perceived control reduces privacy concerns and strengthens adoption intention by providing a sense of autonomy over sensitive information (Tang and Ning, 2023;

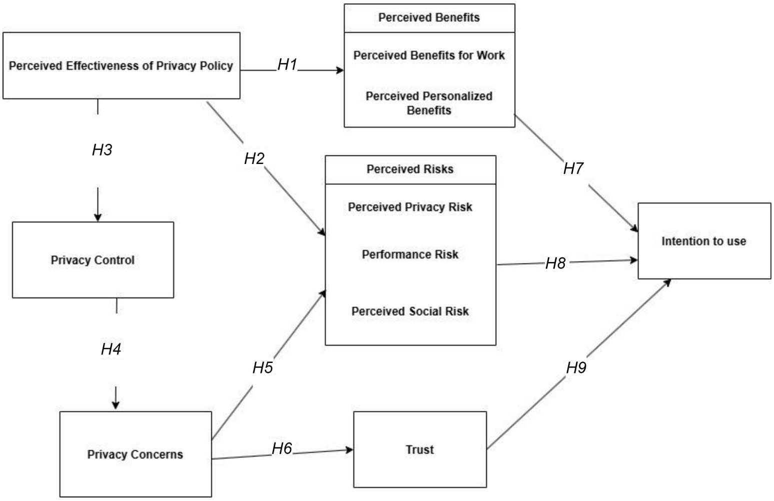

Figure 1. Proposed employee intention assessment model
Source: Authors' own work

Jozani *et al.*, 2020; Ioannou *et al.*, 2020; Wang *et al.*, 2016; Chen *et al.*, 2013; Xu *et al.*, 2011; Malhotra *et al.*, 2004):

H4. Perceived privacy control is negatively associated with privacy concerns.

3.3 Privacy concerns

Privacy concerns refer to employees' belief that using wearables at work may expose their personal data and reduce their control over it (Singh, 2023; Duan and Deng, 2021). Prior research consistently shows that such concerns increase perceived risks and erode trust, acting as a significant barrier to adoption (Sun and Gu, 2024; Duan and Deng, 2021; Liu *et al.*, 2021; Jozani *et al.*, 2020; Ioannou *et al.*, 2020; Guo *et al.*, 2012; Xu *et al.*, 2011; Dinev and Hart, 2006):

H5. Privacy concerns are positively associated with perceived privacy risks.

H6. Privacy concerns are negatively associated with trust.

3.4 Perceived benefits

Perceived benefits are the advantages employees expect from using wearables at work, such as improved productivity, access to information and personalized support. When employees believe that sharing data leads to tangible work-related gains, they are more willing to adopt such technologies (Tang and Ning, 2023; Fox *et al.*, 2021; Sergueeva *et al.*, 2020; Aguirre *et al.*, 2016; Guo *et al.*, 2016; Li *et al.*, 2016; Sutanto *et al.*, 2013; Guo *et al.*, 2012; Junglas and Watson, 2006; Schafer *et al.*, 2001):

H7. Perceived benefits are positively associated with the intention to use a wearable device.

3.5 Perceived risks

Perceived risks capture the negative consequences employees associate with sharing data through wearables, including privacy violations, performance issues and social stigma. When risks are seen as high, employees are less likely to adopt such technologies (Sun and Gu, 2024; Liu *et al.*, 2021; Magni *et al.*, 2021; Jozani *et al.*, 2020; Mohammed and Redzuan, 2020; Li *et al.*, 2019; Li *et al.*, 2016; Yang *et al.*, 2016; Gao *et al.*, 2015; Zhang, *et al.*, 2015; Dinev *et al.*, 2013; Xu *et al.*, 2011; Fensli *et al.*, 2010; Dinev and Hart, 2006):

H8. Perceived risks are negatively associated with the intention to use a wearable device.

3.6 Trust

Trust is a key factor in technology adoption, especially when employees have little prior experience with wearables. Confidence in employers and colleagues reduces uncertainty and facilitates acceptance, making employees more willing to adopt such devices (Tang and Ning, 2023; Magni *et al.*, 2021; Mohammed and Redzuan, 2020; Santoro *et al.*, 2020; Asadi *et al.*, 2019; Miltgen and Smith, 2019; Khasawneh, 2018; Kalantari, 2017; Lin *et al.*, 2015; Guo *et al.*, 2012; Komiak and Benbasat, 2006; Jarvenpaa *et al.*, 1999):

H9. Trust is positively associated with the intention to use a wearable device.

4. Methods

A structured questionnaire was developed to measure employees' intention to adopt workplace wearables, following approval from the University Ethics and Deontology Committee. The questionnaire comprised two sections:

(1) demographic and job related information; and

(2) items measuring the seven research constructs.

A total of 37 items, adapted from validated scales in prior studies (Table 1), were rated on a five-point Likert scale (1 = strongly disagree, 5 = strongly agree). The questionnaire items were adapted to the workplace wearable context to ensure content validity, while the full instrument is provided in the Appendix.

Table 1. Questionnaire composition and origins

Factors	No. of items	References
Perceived effectiveness of privacy policy	3	Xu *et al.*, 2008
Privacy control	4	Xu, 2007
Privacy concerns	4	Dinev and Hart, 2006
Perceived benefits	6	Fox *et al.*, 2021; Li *et al.*, 2016; Xu *et al.*, 2011
Perceived risks	10	Yang *et al.*, 2016; Verdegem and De Marez, 2011; Malhotra *et al.*, 2004; Jarvenpaa *et al.*, 1999; Stone and Grønhaug, 1993
Trust	6	Magni *et al.*, 2021; Gu *et al.*, 2009
Intention to use	4	Li *et al.*, 2019; Pan and Jordan-Marsh, 2010
Total number of items	37	

Source(s): Authors' own work

To ensure clarity and accuracy, the questionnaire was translated into Greek following a forward-backward translation procedure. Prior to distribution, a pilot study was conducted with a small group of participants to assess clarity and identify potential ambiguities. Minor revisions were subsequently made to improve the wording of selected items. In addition, the instrument included definitions and visual examples (e.g. VR and EEG headsets) to facilitate respondents' understanding (Jacobs *et al.*, 2019; Li *et al.*, 2019).

The questionnaire was distributed online via Google Forms between July and October 2024. A convenience sampling approach was used, and participants were recruited through professional networks (e.g. LinkedIn contacts) and online distribution channels, including social media and email sharing. Eligibility required participants to be over 18 years old and currently employed in Greece. Participation was voluntary and anonymous, and the confidentiality of all responses was ensured. A total of 2,305 responses were collected.

Data screening procedures were applied to ensure data quality. Responses were examined for completeness and consistency, and no substantial missing data were identified. Outliers were detected using the Mahalanobis Distance Test ($p < 0.002$ based on χ^2 distribution and model degrees of freedom), resulting in the removal of 62 cases and a final sample of 2,243 participants.

The data were analyzed using SPSS and AMOS, and the structural model was estimated using Maximum Likelihood (ML). The assumptions underlying Maximum Likelihood estimation, including multivariate normality and sample adequacy, were assessed prior to model estimation.

In addition to the hypothesized model, several additional paths were identified after the initial model estimation. These relationships are treated as post hoc modifications and are reported as exploratory. Their inclusion is supported by theoretical reasoning and prior literature.

5. Results

5.1 Descriptive statistics

Table 2 summarizes the demographic and occupational characteristics of the participants. Most employees who participated in the survey belong to the age group 36–50 (31.2%), while the remaining age groups show relatively similar proportions, ranging between 22% and 24.4%. Almost half of the participants (46.5%) held a university degree, while 28.6% had completed postgraduate studies and 24.9% had completed secondary education. Regarding professional experience, 43.6% of employees have more than 15 years of experience, indicating a highly experienced sample. In contrast, 23.8% have 1–5 years of experience, while smaller proportions are observed for those with less than one year (9.7%), 6–10 years (13.1%) and 11–15 years (9.9%).

Regarding organizational tenure, 31.1% of participants had worked in their current company for 1–5 years, while 27.9% has remained with the same employer for more than 15 years. The remaining participants reported organizational tenure of less than one year (18.8%), 6–10 years (12.8%) or 11–15 years (7.4%). Regarding tenure in their current position, 34.1% had held the same position for 1–5 years, 25.1% for more than 15 years and 18.8% for less than a year.

Most participants were employed in the service sector (39.6%), followed by industry/crafts (24.6%). Smaller proportions worked in trade (13.5%), construction (8.7%), tourism (7.0%) and banking (6.6%).

Beyond demographics, participants were also asked about their familiarity and perceptions regarding wearable devices such as VR and EEG headsets. Awareness was generally limited: nearly half (47%) reported no prior knowledge, 42.8% had only general awareness and 7.5% had accessed information through reading or videos. Only a very small proportion (2.7%) had prior hands-on experience. Despite this low level of direct exposure, attitudes toward

Table 2. Results of descriptive questions

Demographics	Categories	Frequency	%
Age group	18–25	503	22.4
	26–35	494	22
	36–50	699	31.2
	50+	547	24.4
Education	Secondary	560	24.9
	University degree	1,043	46.5
	Postgraduate degree	640	28.6
Experience in years	< 1	218	9.7
	1–5	533	23.8
	6–10	292	13.1
	11–15	221	9.9
	15+	979	43.6
Years in current company	< 1	444	19.8
	1–5	719	32.1
	6–10	287	12.8
	11–15	167	7.4
	15+	626	27.9
Years in current position	< 1	421	18.8
	1–5	764	34.1
	6–10	316	14.1
	11–15	180	8
	15+	562	25.1
Industry sector	Industrial/Manufacturing	552	24.6
	Construction	196	8.7
	Tourism	156	7
	Trade	303	13.5
	Services	887	39.6
	Banks	149	6.6

Source(s): Authors' own work

workplace use were cautiously positive: 60.8% stated they would be willing to use such devices in some processes, while 39.2% expressed reluctance.

Expectations regarding productivity varied across respondents. A notable proportion of respondents (24.7%) anticipated a slight productivity improvement, while 18.7% expected a moderate improvement and 12% a significant increase. By contrast, 26.7% believed their productivity would remain unaffected, and 17.9% expected it to decline. Table 3 shows that, despite limited familiarity, a considerable proportion of employees expressed willingness to use wearable technologies under appropriate conditions.

5.2 Factor analysis and discriminant validity analysis

To assess validity and reliability, a factor analysis was conducted using the indicators in Table 4. The KMO index exceeded 0.50 and Bartlett's test was significant ($p < 0.001$). TVE values were above 60% for all factors. Factor loadings were above 0.50 and Cronbach's α exceeded 0.70 (Fabrigar and Wegener, 2012; Thompson, 2004).

Discriminant validity was assessed using Fornell–Larcker criterion (Fornell and Larcker, 1981). The square root of AVE for each factor exceeded its highest correlation with other constructs, indicating satisfactory discriminant validity (Table 5).

Table 3. Perceptions and awareness of wearable devices

Question	Categories	Frequency	%
Did you know before you participated in the survey about the existence of wearable devices like VR, EEG, etc.?	Yes, but I didn't know that many details	960	42.8
	Yes, I have read and seen videos about this device	169	7.5
	Yes, I have used such a device	60	2.7
	No, I was not aware of their existence	1,054	47
Would you use such a device in the context of your work?	Yes, I would use it in some processes	1,364	60.8
	No, I wouldn't use it	879	39.2
How do you think using these devices would affect your productivity?	It won't affect my productivity	600	26.7
	It will slightly improve my productivity	553	24.7
	It will moderately improve my productivity	419	18.7
	It will significantly improve my productivity	270	12
	It will reduce my productivity	401	17.9

Source(s): Authors' own work

Table 4. Factor analysis

Factor	Mean	SD	KMO	Bartlett's sig	TVE	Cronbach α	Loadings	CR	AVE
Privacy concerns	3.53	0.92	0.83	< 0.001	74.82	0.89	> 0.79	0.92	0.75
Privacy control	2.65	0.94	0.85	< 0.001	84.11	0.94	> 0.89	0.96	0.84
Perceived effectiveness of privacy policy	3.31	0.91	0.74	< 0.001	86.45	0.92	> 0.90	0.95	0.86
Perceived risks									
Perceived privacy risk	3.39	0.80	0.82	< 0.001	76.37	0.90	> 0.85	0.93	0.76
Performance risk	3.30	0.74	0.70	< 0.001	66.91	0.75	> 0.82	0.86	0.67
Perceived social risk	2.87	1.01	0.75	< 0.001	81.56	0.89	> 0.89	0.93	0.82
Trust	3.45	0.75	0.82	< 0.001	67.63	0.90	> 0.75	0.93	0.68
Perceived benefits									
Perceived benefits for work	3.41	0.78	0.72	< 0.001	80.64	0.88	> 0.86	0.93	0.81
Perceived personalized benefits	3.67	0.73	0.74	< 0.001	85.53	0.92	> 0.91	0.95	0.86
Intention to use	3.10	0.85	0.83	< 0.001	80.73	0.92	> 0.87	0.95	0.81

Source(s): Authors' own work

Descriptive statistics indicate that employees express moderate to high concern ($\mu = 3.53$) about providing data to wearable devices and about issues of excessive data collection and use for unknown purposes. Furthermore, employees state that they have limited control over their personal data ($\mu = 2.65$), as they feel that they do not control the type of data that wearable devices collect but also cannot adequately manage who has access to their data. Regarding employees' perception of the effectiveness of the privacy policy of the company they work for, they believe that there is respect for their personal data and that to a certain extent they will remain confidential given the moderate positive attitude ($\mu = 3.31$).

Table 5. Discriminant validity (Fornell–Larcker criterion)

Factor	Privacy concerns	Privacy control	Perceived effectiveness of privacy policy	Perceived privacy risk	Performance risk	Trust	Perceived social risk	Perceived benefits for work	Perceived personalized benefits	Intention to use
Privacy concerns	0.865									
Privacy control	−0.314	0.917								
Perceived effectiveness of privacy policy	−0.168	0.491	0.930							
Perceived privacy risk	0.507	−0.240	−0.192	0.874						
performance risk	0.396	−0.198	−0.121	0.512	0.818					
Trust	−0.133	0.326	0.519	−0.162	−0.111	0.903				
Perceived social risk	0.199	−0.080	−0.103	0.229	0.276	−0.162	0.822			
Perceived benefits for work	−0.086	0.279	0.342	−0.161	−0.181	0.347	−0.134	0.898		
Perceived personalized benefits	0.084	0.145	0.263	−0.057		0.300	−0.060	0.514	0.925	
Intention to use	−0.242	0.447	0.367	−0.293	−0.270	0.390	0.148	0.601	0.392	0.898

Source(s): Authors' own work

Perceived risk was moderate to high, particularly with respect to privacy and performance risks. Respondents expressed concerns about potential data disclosure, uncertainty, loss of privacy and the possibility of unexpected problems ($\mu = 3.39$). They also reported moderate concern regarding the performance of wearable devices, including whether these technologies would deliver the expected benefits and provide accurate and reliable results ($\mu = 3.30$). In contrast, perceived social risk was lower ($\mu = 2.87$), indicating relatively limited concern about colleagues' perceptions of wearable device use.

Perceived benefits were rated at a moderate to positive level ($\mu = 3.41$). Participants believed that wearable technologies could provide personalized services tailored to their needs and interests, while productivity-related benefits received an even higher rating ($\mu = 3.67$), particularly regarding productivity enhancement, improved access to information and the quality of work processes. Trust in the workplace was also moderate to positive ($\mu = 3.45$). Participants generally perceived their employer and colleagues as trustworthy and reported feeling reasonably confident when encouraged to use wearable devices, although some reservations remained.

Overall, employees reported a moderate intention to adopt wearable technologies ($\mu = 3.10$), suggesting cautious acceptance under appropriate conditions.

5.3 Structural equation model

The structural model (Figure 2) explained 46% of the variance in employees' intention to use wearable devices. The results indicate that perceived benefits have the largest impact (0.42/*H7*) on intention to use, followed by perceived control (0.25), perceived concerns (−0.10) and trust (0.09/*H9*).

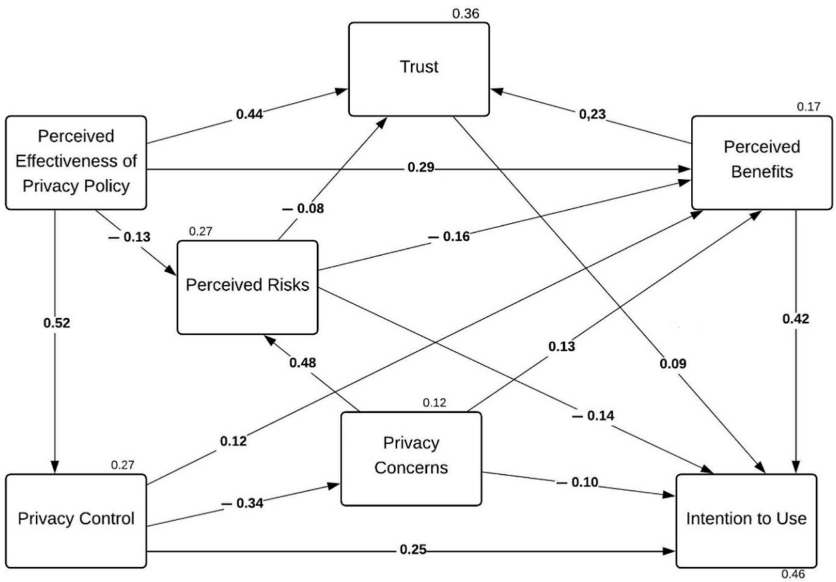

Figure 2. Structural equation model results

Note: Values on the paths represent standardized regression coefficients (β), while R^2 values indicate the explained variance of the endogenous variables

Source: Authors' own work

The fit indices of the model are listed in Table 6, where the values indicate that the model under analysis is of good fit. All indices are within or beyond the acceptable limits, concluding that the model describes the data well with high accuracy and is suitable for interpretation. Table 7 reports the findings regarding the research hypotheses but also lists the new relationships between the factors that emerged after the statistical analysis.

6. Discussion

6.1 Direct and indirect effects of the model factors

Table 8 summarizes the direct, indirect and total effects among the research factors of the model. The effectiveness of the privacy policy plays a central role in the model, as it is linked either directly or indirectly to the other factors. More specifically, the effectiveness of the company's privacy policy directly affects privacy control (r = 0.517) and indirectly affects privacy concerns ($r = -0.177$). Previous studies have similarly shown that effective organizational privacy policies enhance employees' perceived control while reducing privacy concerns (Zhang *et al.*, 2025; Tang and Ning, 2023;

Table 6. Model fit indices

Indices	x^2/df	GFI	CFI	RMSEA	RMR
Scores	2.145	0.999	0.999	0.023	0.007

Source(s): Authors' own work

Table 7. Hypothesis testing

Hypothesis	Hypothesis testing Path	Result
H1	Perceived effectiveness of privacy policy → Perceived benefits	Accepted
H2	Perceived effectiveness of privacy policy → Perceived risks	Accepted
H3	Perceived effectiveness of privacy policy → Privacy control	Accepted
H4	Privacy control → Privacy concerns	Accepted
H5	Privacy concerns → Perceived risks	Accepted
H6	Privacy concerns → Trust	Rejected
H7	Perceived benefits → Intention to use	Accepted
H8	Perceived risks → Intention to use	Accepted
H9	Trust → Intention to use	Accepted
New proposed paths		
Perceived effectiveness of privacy policy → Trust		
Perceived benefits → Trust		
Perceived risks → Perceived benefits		
Privacy control → Perceived benefits		
Privacy concerns → Perceived benefits		
Privacy concerns → Intention to use		
Perceived risks → Trust		
Privacy control → Intention to use		

Note(s): All supported hypotheses are significant at $p < 0.001$
Source(s): Authors' own work

Table 8. Direct and indirect effects of the model factors

Factor	Perceived effectiveness of privacy policy	Privacy control	Privacy concerns	Perceived risks	Perceived benefits	Trust
Privacy control						
D	0.517					
I						
T	*0.517*					
Privacy concerns						
D		−0.343				
I	−0.177					
T	*−0.177*	*−0.343*				
Perceived risks						
D	−0.133		0.481			
I	−0.085	−0.165				
T	*−0.218*	*−0.165*	*0.481*			
Perceived benefits						
D	0.294	0.122	0.135	−0.163		
I	0.075	−0.019	−0.079			
T	*0.369*	*0.103*	*0.056*	*−0.163*		
Trust						
D	0.444			−0.080	0.233	
I	0.103	0.037	−0.025	−0.038		
T	*0.548*	*0.037*	*−0.025*	*−0.118*	*0.233*	
Intention to use						
D		0.247	−0.100	−0.136	0.424	0.093
I	0.382	0.104	−0.044	−0.080	0.022	
T	*0.382*	*0.351*	*−0.144*	*−0.216*	*0.446*	*0.093*

Source(s): Authors' own work

Liu *et al.*, 2021; Mutimukwe *et al.*, 2020; Xu *et al.*, 2011). When a company's privacy policy is effective, employees feel in control of who has access to the data they provide on their wearable devices and the type of data collected. Consequently, employees become less concerned about how their personal data are collected, accessed and used within the organization.

Privacy policy effectiveness also negatively impacts perceived risks ($r = -0.218$), positively impacts perceived benefits ($r = 0.369$) and trust ($r = 0.548$). These findings are consistent with previous research (Aluri, 2025; Liu *et al.*, 2021; Mutimukwe *et al.*, 2020; Wang *et al.*, 2020; Xu *et al.*, 2011). A clear and transparent privacy policy increases perceived benefits, strengthens trust in the organization and reduces employees' perceived risks associated with workplace wearables. Consequently, it indirectly promotes employees' intention to use wearable devices ($r = 0.382$), highlighting the central role of privacy policy effectiveness in workplace technology adoption (Liu *et al.*, 2021). This finding is also consistent with recent research suggesting that transparent governance, participatory HRM practices and organizational governance mechanisms can mitigate the negative consequences of workplace surveillance while strengthening workplace trust employees' acceptance of digital monitoring technologies (Kayas *et al.*, 2025; Patel *et al.*, 2026).

Perceived control appears to influence four of the five remaining factors. The negative influence of perceived control on employees' privacy concerns ($r = -0.343$) is consistent with findings in the literature (Liu *et al.*, 2021) and is due to the fact that the more control they have over the data provided on wearable devices, the less they worry about their use for purposes they do not know and the lack of protection in the company's databases (Virgillito *et al.*, 2025). In addition, perceived control has a positive influence on perceived benefits ($r = 0.103$) and a negative influence on perceived risks ($r = -0.165$). Previous research has likewise shown that greater perceived control enhances perceived benefits while reducing perceived risks (Atalay and Yücel, 2024; Mutimukwe *et al.*, 2020).

Examining the effect of control on employees' trust in colleagues and employer and ultimately on the intention to provide data to wearable devices, $r = 0.037$ and $r = 0.351$ are obtained, respectively. Perceived control has a small, positive effect on trust, while a fairly strong, positive effect on adoption intention. These findings suggest that employees who perceive greater control over their personal data are more willing to adopt wearable technologies in organizational settings (Atalay and Yücel, 2024).

Regarding employee privacy concerns, they seem to have a positive and strong effect on perceived risks ($r = 0.481$) and a slightly positive effect on perceived benefits ($r = 0.056$). Previous studies consistently report that the relationship between these factors and conclude that the more privacy concerns increase, the more perceived risks employees will face (Tang and Ning, 2023; Fox *et al.*, 2021; Liu *et al.*, 2021; Jozani *et al.*, 2020). Regarding the effect of privacy concerns on trust, the relationship is slightly negative ($r = -0.025$) and not statistically significant. In contrast, privacy concerns have a moderate and negative effect on intention to use ($r = -0.144$). These findings suggest that while privacy concerns do not appear to substantially influence trust in the workplace, they are associated with a lower intention to adopt wearable devices. This is consistent with prior research indicating that increased concerns about personal data may reduce employees' willingness to engage with such technologies (Fox *et al.*, 2021; Sergueeva *et al.*, 2020; Guo *et al.*, 2012). Similarly, recent evidence suggests that employees exposed to workplace monitoring technologies report less positive workplace attitudes when surveillance practices are perceived as intrusive or insufficiently transparent (Abrams *et al.*, 2026).

In this context, the effect of perceived risks on perceived benefits ($r = -0.163$), trust ($r = -0.118$) and overall intention to use ($r = -0.216$) was also measured. Perceived risks have a moderately negative effect on all three factors. These findings suggest that the more risks they perceive that using a wearable device and providing data to it has, the fewer the perceived benefits, the less trust they show in employees and employers, and overall they are less likely to adopt such technologies (Ali *et al.*, 2021; Magni *et al.*, 2021; Mohammed and Redzuan, 2020; Park *et al.*, 2019; Li *et al.*, 2016; Gao *et al.*, 2015). Regardless of whether these risks relate to privacy, social, or performance issues, their overall influence on adoption intention remains negative.

Trust directly and positively influences ($r = 0.233$) employees' perceived benefits, a finding that is consistent with previous research linking trust to intention to use (Ali *et al.*, 2021; Park *et al.*, 2019). Employees' trust in their employer and colleagues leads them to face the situation with optimism and perceive more benefits. In turn, perceived benefits significantly influence ($r = 0.446$) their intention to adopt a wearable device during work (Fox *et al.*, 2021; Park *et al.*, 2019). For the above reasons, a small direct effect of trust on intention to use is observed ($r = 0.093$), which is not statistically significant (Ali *et al.*, 2021; Magni *et al.*, 2021; Mohammed and Redzuan, 2020; Guo *et al.*, 2012).

It should be noted that the additional structural relationships incorporated into the final model represent exploratory post hoc modifications identified after the initial model estimation. Although these relationships are supported by prior literature and contributed to an improved model fit, they were not part of the original conceptual model. Therefore, they should be interpreted with caution and validated in future studies using independent samples.

7. Conclusion

The proposed framework enhances understanding of the factors influencing employees' intention to adopt wearable devices in the workplace. It focuses on wearable technologies that monitor and collect physical, cognitive or emotional data and contributes to the literature by providing evidence from a relatively underexplored context, where organizational adoption of wearable devices remains limited.

In addition, the study extends prior research by applying Privacy Calculus Theory in an organizational setting, offering an alternative perspective to commonly used technology acceptance models. Given that most participants had limited direct experience with wearable devices, this approach allows for a more appropriate examination of perceived risks, benefits and privacy-related considerations.

The findings indicate that the model explains 46% of the variance in intention to use. Among the examined factors, perceived benefits, privacy policy effectiveness and perceived control show stronger associations with intention to use, while other relationships are weaker or not statistically significant. These findings highlight the multifaceted nature of employees' decision-making regarding wearable adoption.

Overall, the findings suggest that while perceived benefits play an important role in shaping adoption intentions, concerns and perceived risks may act as barriers. Organizational mechanisms such as transparent privacy policies and enhanced employee control appear to contribute to balancing these opposing forces, supporting the responsible and acceptable integration of wearable technologies in the workplace.

7.1 Practical implications

The study's findings provide practical guidance for organizations considering the integration of wearable technologies into workplace processes. Addressing employees' concerns about data privacy and security is essential for the successful adoption of such technologies in areas such as recruitment, performance monitoring and training (Fox *et al.*, 2021). Organizations can benefit from strategies that position wearable technologies as supportive workplace tools, provided that appropriate organizational safeguards are established (Jacobs *et al.*, 2019).

More specifically, these findings can be translated into concrete managerial scenarios. In the context of HR analytics, organizations should ensure that data collected through wearable devices are explicitly linked to employee development and performance improvement, rather than perceived as tools for surveillance. In occupational safety, wearables can be used to monitor fatigue, stress, or exposure to risks, provided that employees are clearly informed about the purpose, scope and limits of data collection. In productivity monitoring, transparency regarding how data are interpreted and used in evaluation processes is critical to avoid resistance and mistrust. Similarly, in training and development, wearable technologies (e.g. VR-based training environments) should be positioned as tools that enhance learning and skill acquisition rather than mechanisms of control.

It is therefore recommended that organizations strengthen the security of employees' personal data and ensure transparency in how data are collected, stored and used. Clear communication of privacy policies, including updates and improvements, can enhance employees' sense of security and foster trust in the organization (Asadi *et al.*, 2019). Given that perceived control significantly influences intention to use, organizations should also enable employees to have a degree of control over the data collected and how they are used (Tang and Ning, 2023).

Employees' concerns and uncertainty may also stem from previous experiences or broader perceptions of digital surveillance. Therefore, organizations should not only inform employees about data protection measures but also demonstrate them in practice. Although trust has only a moderate direct effect on intention to use, it can facilitate the successful integration of wearable technologies into work processes (Magni *et al.*, 2021; Santoro *et al.*, 2020). A supportive organizational environment should include open communication between management and employees, as well as employee participation in discussions and decision-making processes related to the adoption of such technologies. This approach can reduce perceived risks and concerns, including fear of social stigma, thereby limiting their negative impact on adoption decisions.

Finally, managers should leverage employees' perceptions of the benefits associated with wearable technologies, such as improved productivity, personalization and enhanced performance in daily tasks (Sergueeva *et al.*, 2020). However, as highlighted in recent research, a high level of willingness to adopt such technologies does not automatically translate into actual data-sharing behavior or sustained use. Effective implementation requires the development of appropriate policies, mechanisms and user-centered design approaches that can bridge the gap between intention and actual adoption (Chandrasekaran *et al.*, 2025). Therefore, the proposed managerial implications should be viewed as recommendations that support employees' intention to adopt wearable technologies rather than evidence of actual implementation or sustained organizational use.

7.2 Limitations and future research

A key limitation is that the study examines employees' intention to use wearable devices rather than actual usage behavior. Given that most respondents had limited or no prior hands-on experience with such technologies, their responses reflect perceptions and expectations rather than real-world interaction. Therefore, the findings should be interpreted with appropriate caution when generalizing to actual workplace adoption.

In addition, the geographic focus exclusively on Greek workers limits the generalizability of the findings to other countries or cultural settings. Future research could examine additional organizational factors and adopt longitudinal designs to investigate actual wearable technology use in workplace settings over time.

References

Abrams, L., Schneider, D. and Harknett, K. (2026), "New technology, older workers: how workplace technology is associated with indicators of job retention", *Journal of Aging and Social Policy*, Vol. 38 No. 4, pp. 635-651.

Aguirre, E., Roggeveen, A.L., Grewal, D. and Wetzels, M. (2016), "The personalization-privacy paradox: implications for new media", *Journal of Consumer Marketing*, Vol. 33 No. 2, pp. 98-110.

Ajunwa, I., Crawford, K. and Schultz, J. (2017), "Limitless worker surveillance", *California Law Review*, Vol. 105, p. 735.

Al-Emran, M., Al-Nuaimi, M.N., Arpaci, I., Al-Sharafi, M.A. and Anthony Jnr, B. (2023), "Towards a wearable education: understanding the determinants affecting students' adoption of wearable technologies using machine learning algorithms", *Education and Information Technologies*, Vol. 28 No. 3, pp. 2727-2746.

Ali, M., Raza, S.A., Khamis, B., Puah, C.H. and Amin, H. (2021), "How perceived risk, benefit and trust determine user fintech adoption: a new dimension for islamic finance", *foresight*, Vol. 23 No. 4, pp. 403-420.

Aluri, A. (2025), "Evaluating privacy trust assurance in the context of utilizing wearable augmented reality business applications among professionals in the hospitality industry", *Journal of Quality Assurance in Hospitality and Tourism*, pp. 1-20.

Asadi, S., Abdullah, R., Safaei, M. and Nazir, S. (2019), "An integrated SEM-neural network approach for predicting determinants of adoption of wearable healthcare devices", *Mobile Information Systems*, Vol. 2019 No. 1, p. 8026042.

Atalay, H.N. and Yücel, Ş. (2024), "Decoding privacy concerns: the role of perceived risk and benefits in personal health data disclosure", *Archives of Public Health*, Vol. 82 No. 1, p. 180.

Ball, K. (2010), "Workplace surveillance: an overview", *Labor History*, Vol. 51 No. 1, pp. 87-106.

Canhoto, A.I. and Arp, S. (2017), "Exploring the factors that support adoption and sustained use of health and fitness wearables", *Journal of Marketing Management*, Vol. 33 Nos 1-2, pp. 32-60.

Chandrasekaran, R., Sadiq T, M. and Moustakas, E. (2025), "Usage trends and data sharing practices of healthcare wearable devices among US adults: cross-sectional study", *Journal of Medical Internet Research*, Vol. 27, p. e63879.

Chen, X., Ma, J., Jin, J. and Fosh, P. (2013), "Information privacy, gender differences, and intrinsic motivation in the workplace", *International Journal of Information Management*, Vol. 33 No. 6, pp. 917-926.

Chuah, S.H.W., Rauschnabel, P.A., Krey, N., Nguyen, B., Ramayah, T. and Lade, S. (2016), "Wearable technologies: the role of usefulness and visibility in smartwatch adoption", *Computers in Human Behavior*, Vol. 65, pp. 276-284.

Cilliers, L. (2020), "Wearable devices in healthcare: Privacy and information security issues", *Health Information Management Journal*, Vol. 49 Nos 2-3, pp. 150-156.

Davis, F.D. (1989), "Technology acceptance model: TAM", *AS: Information Seeking Behavior and Technology Adoption*, Vol. 205 No. 219, p. 5.

Debnath, A., Kobra, K.T., Rawshan, P.P., Paramita, M. and Islam, M.N. (2018), "An explication of acceptability of wearable devices in context of Bangladesh: a user study", in *2018 IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud), Barcelona, Spain, IEEE*, pp. 136-140.

Dinev, T. and Hart, P. (2006), "An extended privacy calculus model for e-commerce transactions", *Information Systems Research*, Vol. 17 No. 1, pp. 61-80.

Dinev, T., Xu, H., Smith, J.H. and Hart, P. (2013), "Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts", *European Journal of Information Systems*, Vol. 22 No. 3, pp. 295-316.

Duan, S.X. and Deng, H. (2021), "Hybrid analysis for understanding contact tracing apps adoption", *Industrial Management and Data Systems*, Vol. 121 No. 7, pp. 1599-1616.

Dwivedi, Y.K., Rana, N.P., Jeyaraj, A., Clement, M. and Williams, M.D. (2019), "Re-examining the unified theory of acceptance and use of technology (UTAUT): towards a revised theoretical model", *Information Systems Frontiers*, Vol. 21 No. 3, pp. 719-734.

Fabrigar, L.R. and Wegener, D.T. (2012), *Exploratory Factor Analysis*, Oxford University Press.

Felea, M., Bucur, M., Negruțiu, C., Nitu, M. and Stoica, D.A. (2021), "Wearable technology adoption among romanian students: a structural model based on TAM", *Amfiteatru Economic*, Vol. 23 No. 57, pp. 376-391.

Fensli, R., Dale, J.G., O'Reilly, P., O'Donoghue, J., Sammon, D. and Gundersen, T. (2010), "Towards improved healthcare performance: examining technological possibilities and patient satisfaction with wireless body area networks", *Journal of Medical Systems*, Vol. 34 No. 4, pp. 767-775.

Fornell, C. and Larcker, D.F. (1981), "Evaluating structural equation models with unobservable variables and measurement error", *Journal of Marketing Research*, Vol. 18 No. 1, pp. 39-50.

Fox, G., Clohessy, T., van der Werff, L., Rosati, P. and Lynn, T. (2021), "Exploring the competing influences of privacy concerns and positive beliefs on citizen acceptance of contact tracing mobile applications", *Computers in Human Behavior*, Vol. 121, p. 106806.

Gao, Y., Li, H. and Luo, Y. (2015), *An Empirical Study of Wearable Technology Acceptance in Healthcare. Industrial Management and Data Systems*, Vol. 115 No. 9, pp. 1704-1723.

Gu, J.C., Lee, S.C. and Suh, Y.H. (2009), "Determinants of behavioral intention to mobile banking", *Expert Systems with Applications*, Vol. 36 No. 9, pp. 11605-11616.

Guo, X., Sun, Y., Yan, Z. and Wang, N. (2012), "Privacy-personalization paradox in adoption of mobile health service: the mediating role of trust".

Guo, X., Zhang, X. and Sun, Y. (2016), "The privacy–personalization paradox in mHealth services acceptance of different age groups", *Electronic Commerce Research and Applications*, Vol. 16, pp. 55-65.

Hellenic Statistical Authority (ELSTAT) (2023), "Information and communication technologies (ICT) usage survey in households and by individuals", available at: www.statistics.gr/documents/20181/1c86d4da-d94e-f6f0-5f1e-5caa6ff46435

Howe, J., Kariotis, T., Bromberg, L. and Fagan, J. (2026), "Is the boss watching, and are unions doing anything about it? Workplace surveillance regulation in Australian enterprise agreements", *Labour and Industry*, Vol. 36 No. 1, pp. 25-47.

Ioannou, A., Tussyadiah, I. and Lu, Y. (2020), "Privacy concerns and disclosure of biometric and behavioral data for travel", *International Journal of Information Management*, Vol. 54, p. 102122.

Jacobs, J.V., Hettinger, L.J., Huang, Y.H., Jeffries, S., Lesch, M.F., Simmons, L.A., Verma, S.K. and Willetts, J.L. (2019), "Employee acceptance of wearable technology in the workplace", *Applied Ergonomics*, Vol. 78, pp. 148-156.

Jarvenpaa, S.L., Tractinsky, N. and Saarinen, L. (1999), "Consumer trust in an internet store: a cross-cultural validation", *Journal of Computer-Mediated Communication*, Vol. 5 No. 2, p. JCMC526.

Jozani, M., Ayaburi, E., Ko, M. and Choo, K.K.R. (2020), "Privacy concerns and benefits of engagement with social media-enabled apps: a privacy calculus perspective", *Computers in Human Behavior*, Vol. 107, p. 106260.

Jung, Y., Kim, S. and Choi, B. (2016), "Consumer valuation of the wearables: the case of smartwatches", *Computers in Human Behavior*, Vol. 63, pp. 899-905.

Junglas, I. and Watson, R.T. (2006), "The u-constructs: four information drives", *Communications of the Association for Information Systems*, Vol. 17 No. 1, p. 26.

Kalantari, M. (2017), "Consumers' adoption of wearable technologies: literature review, synthesis, and future research agenda", *International Journal of Technology Marketing*, Vol. 12 No. 3, pp. 274-307.

Kayas, O.G., Ong, C.E. and Belal, H.M. (2025), "From humans to algorithms: a sociotechnical framework of workplace surveillance", *Digital Business*, Vol. 5 No. 2, p. 100120.

Kellogg, K.C., Valentine, M.A. and Christin, A. (2020), "Algorithms at work: the new contested terrain of control", *Academy of Management Annals*, Vol. 14 No. 1, pp. 366-410.

Kerner, C. and Goodyear, V.A. (2017), "The motivational impact of wearable healthy lifestyle technologies: a self-determination perspective on fitbits with adolescents", *American Journal of Health Education*, Vol. 48 No. 5, pp. 287-297.

Khakurel, J., Melkas, H. and Porras, J. (2018), "Tapping into the wearable device revolution in the work environment: a systematic review", *Information Technology and People*, Vol. 31 No. 3, pp. 791-818.

Khakurel, J., Pöysä, S. and Porras, J. (2017), The use of wearable devices in the workplace-a systematic literature review. In *Smart Objects and Technologies for Social Good: Second International Conference, GOODTECHS 2016, Venice, Italy*, November 30–December 1, *Springer International Publishing*, Vol. 2, pp. 284-294.

Khasawneh, O.Y. (2018), "Technophobia without boarders: the influence of technophobia and emotional intelligence on technology acceptance and the moderating influence of organizational climate", *Computers in Human Behavior*, Vol. 88, pp. 210-218.

Kim, K.J. and Shin, D.H. (2015), "An acceptance model for smart watches: Implications for the adoption of future wearable technology", *Internet Research*, Vol. 25 No. 4, pp. 527-541.

Kim, T. and Chiu, W. (2019), "Consumer acceptance of sports wearable technology: the role of technology readiness", *International Journal of Sports Marketing and Sponsorship*, Vol. 20 No. 1, pp. 109-126.

Komiak, S.Y. and Benbasat, I. (2006), "The effects of personalization and familiarity on trust and adoption of recommendation agents", *MIS Quarterly*, Vol. 30 No. 4, pp. 941-960.

Lee, J., Kim, D., Ryoo, H.Y. and Shin, B.S. (2016), "Sustainable wearables: Wearable technology for enhancing the quality of human life", *Sustainability*, Vol. 8 No. 5, p. 466.

Li, H., Wu, J., Gao, Y. and Shi, Y. (2016), "Examining individuals' adoption of healthcare wearable devices: an empirical study from privacy calculus perspective", *International Journal of Medical Informatics*, Vol. 88, pp. 8-17.

Li, J., Ma, Q., Chan, A.H. and Man, S. (2019), "Health monitoring through wearable technologies for older adults: Smart wearables acceptance model", *Applied Ergonomics*, Vol. 75, pp. 162-169.

Liang, R.Y., Li, Y. and Wei, W. (2024), "Advancing elderly healthcare: adapting UTAUT2 with inhibitors for wearable device continuance", *Library Hi Tech*, Vol. 43 Nos 2-3.

Lin, C.H., Shih, H.Y. and Sher, P.J. (2007), "Integrating technology readiness into technology acceptance: the TRAM model", *Psychology and Marketing*, Vol. 24 No. 7, pp. 641-657.

Lin, C.P., Tsai, Y.H., Chiu, C.K. and Liu, C.P. (2015), "Forecasting the purchase intention of IT product: Key roles of trust and environmental consciousness for IT firms", *Technological Forecasting and Social Change*, Vol. 99, pp. 148-155.

Lismont, J., Vanthienen, J., Baesens, B. and Lemahieu, W. (2017), "Defining analytics maturity indicators: a survey approach", *International Journal of Information Management*, Vol. 37 No. 3, pp. 114-124.

Liu, Y.L., Yan, W. and Hu, B. (2021), "Resistance to facial recognition payment in China: the influence of privacy-related factors", *Telecommunications Policy*, Vol. 45 No. 5, p. 102155.

Lunney, A., Cunningham, N.R. and Eastin, M.S. (2016), "Wearable fitness technology: a structural investigation into acceptance and perceived fitness outcomes", *Computers in Human Behavior*, Vol. 65, pp. 114-120.

Magni, D., Scuotto, V., Pezzi, A. and Del Giudice, M. (2021), "Employees' acceptance of wearable devices: towards a predictive model", *Technological Forecasting and Social Change*, Vol. 172, p. 121022.

Malhotra, N.K., Kim, S.S. and Agarwal, J. (2004), "Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model", *Information Systems Research*, Vol. 15 No. 4, pp. 336-355.

Mendoza, J.A., Baker, K.S., Moreno, M.A., Whitlock, K., Abbey-Lambertz, M., Waite, A., Waite, A., Colburn, T. and Chow, E.J. (2017), "A fitbit and facebook mHealth intervention for promoting physical activity among adolescent and young adult childhood cancer survivors: a pilot study", *Pediatric Blood and Cancer*, Vol. 64 No. 12, p. e26660.

Milne, G.R. and Culnan, M.J. (2004), "Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices", *Journal of Interactive Marketing*, Vol. 18 No. 3, pp. 15-29.

Miltgen, C.L. and Smith, H.J. (2019), "Falsifying and withholding: exploring individuals' contextual privacy-related decision-making", *Information and Management*, Vol. 56 No. 5, pp. 696-717.

Mohammed, Z. and Redzuan, F. (2020), "Parent's acceptance on wearable technology for children's safety", *Indonesian Journal of Electrical Engineering and Computer Science*, Vol. 17 No. 2, pp. 1066-1073.

Moore, P.V. (2017), *The Quantified Self in Precarity: Work, Technology and What Counts*, Routledge.

Mutimukwe, C., Kolkowska, E. and Grönlund, Å. (2020), "Information privacy in e-service: Effect of organizational privacy assurances on individual privacy concerns, perceptions, trust and self-disclosure behavior", *Government Information Quarterly*, Vol. 37 No. 1, p. 101413.

Nalchigar, S. and Yu, E. (2018), "Business-driven data analytics: a conceptual modeling framework", *Data and Knowledge Engineering*, Vol. 117, pp. 359-372.

Ng, K., Tynjälä, J. and Kokko, S. (2017), "Ownership and use of commercial physical activity trackers among finnish adolescents: cross-sectional study", *JMIR mHealth and uHealth*, Vol. 5 No. 5, p. e6940.

Pan, S. and Jordan-Marsh, M. (2010), "Internet use intention and adoption among chinese older adults: from the expanded technology acceptance model perspective", *Computers in Human Behavior*, Vol. 26 No. 5, pp. 1111-1119.

Park, J., Amendah, E., Lee, Y. and Hyun, H. (2019), "M-payment service: Interplay of perceived risk, benefit, and trust in service adoption", *Human Factors and Ergonomics in Manufacturing and Service Industries*, Vol. 29 No. 1, pp. 31-43.

Patel, P.C., Rofcanin, Y., Kamasak, R. and Belitski, M. (2026), "Visibility by design: how HRM architectural choices shape workplace relationships in digitally surveilled environments", *Human Resource Management Journal*, doi: 10.1111/1748-8583.70053

Pawirosumarto, S. and Kurniawan, B. (2026), "Datafied selves at work: Ethical boundaries of surveillance in people analytics", *Journal of Business Ethics*, pp. 1-17.

Qureshi, F., Shah, S., Khan, M. and Shaikh, H. (2026), "Artificial intelligence, employee surveillance, and workplace trust: Redefining human resource management in the era of digital transformation", *Journal of Psychology, Health and Social Challenges*, Vol. 4 No. 2, pp. 65-72.

Rahman, M.S., Das, S., Hossain, G.M.S. and Tajrin, T. (2022), "Teenagers' behavioural intention towards wearable technologies and intention to recommend others: an empirical study in Bangladesh", *Journal of Science and Technology Policy Management*, Vol. 13 No. 1, pp. 110-131.

Ren, T., Le, H.T. and Park, J. (2023), "Drivers of customers' efforts to cope with wearable device usage problems and the role of demographics in a study in China", *Asia Pacific Journal of Marketing and Logistics*, Vol. 35 No. 11, pp. 2727-2747.

Rogers, K.E. and Park, J. (2016), "Diy consumers and wearable electronics: What factors affect technology adoption?", In *International Textile and Apparel Association Annual Conference Proceedings*, IA State University Digital Press, Vol. 73, p. 1.

Rowe, F. (2020), "Contact tracing apps and values dilemmas: a privacy paradox in a neo-liberal world", *International Journal of Information Management*, Vol. 55, p. 102178.

Santoro, G., Quaglia, R., Pellicelli, A.C. and De Bernardi, P. (2020), "The interplay among entrepreneur, employees, and firm level factors in explaining SMEs openness: a qualitative micro-foundational approach", *Technological Forecasting and Social Change*, Vol. 151, p. 119820.

Schafer, J.B., Konstan, J.A. and Riedl, J. (2001), "E-commerce recommendation applications", *Data Mining and Knowledge Discovery*, Vol. 5 Nos 1-2, pp. 115-153.

Sergueeva, K., Shaw, N. and Lee, S.H.(. (2020), "Understanding the barriers and factors associated with consumer adoption of wearable technology devices in managing personal health", *Canadian Journal of Administrative Sciences / Revue Canadienne Des Sciences De L'Administration*, Vol. 37 No. 1, pp. 45-60.

Shafique, M.N., Khurshid, M.M., Rahman, H., Khanna, A., Gupta, D. and Rodrigues, J.J. (2019), "The role of wearable technologies in supply chain collaboration: a case of pharmaceutical industry", *IEEE Access*, Vol. 7, pp. 49014-49026.

Shen, S., Xu, K., Sotiriadis, M. and Wang, Y. (2022), "Exploring the factors influencing the adoption and usage of augmented reality and virtual reality applications in tourism education within the context of COVID-19 pandemic", *Journal of Hospitality, Leisure, Sport and Tourism Education*, Vol. 30, p. 100373.

Singh, S. (2023), "The moderating role of privacy concerns on intention to use smart wearable technologies: an integrated model combining UTAUT2 theoretical framework and privacy dimensions", *Journal of Global Marketing*, Vol. 36 No. 2, pp. 93-111.

Stone, R.N. and Grønhaug, K. (1993), "Perceived risk: Further considerations for the marketing discipline", *European Journal of Marketing*, Vol. 27 No. 3, pp. 39-50.

Sun, H. and Gu, C. (2024), "Understanding determinants of end-user's continuance intention on fitness wearable technology", *International Journal of Human–Computer Interaction*, Vol. 40 No. 3, pp. 537-557.

Sutanto, J., Palme, E., Tan, C.H. and Phang, C.W. (2013), "Addressing the personalization-privacy paradox: an empirical assessment from a field experiment on smartphone users", *MIS Quarterly*, Vol. 37 No. 4, pp. 1141-1164.

Tang, Y. and Ning, X. (2023), "Understanding user misrepresentation behavior on social apps: the perspective of privacy calculus theory", *Decision Support Systems*, Vol. 165, p. 113881.

Tavares, J. and Oliveira, T. (2018), "New integrated model approach to understand the factors that drive electronic health record portal adoption: cross-sectional national survey", *Journal of Medical Internet Research*, Vol. 20 No. 11, p. e11032.

Thompson, B. (2004), *Exploratory and Confirmatory Factor Analysis: Understanding Concepts and Applications*, Sage Publications, Washington, DC, p. 3.

Trepte, S., Scharkow, M. and Dienlin, T. (2020), "The privacy calculus contextualized: the influence of affordances", *Computers in Human Behavior*, Vol. 104, p. 106115.

Turhan, G. (2013), "An assessment towards the acceptance of wearable technology to consumers in Turkey: the application to smart bra and t-shirt products", *Journal of the Textile Institute*, Vol. 104 No. 4, pp. 375-395.

Verdegem, P. and De Marez, L. (2011), "Rethinking determinants of ICT acceptance: towards an integrated and comprehensive overview", *Technovation*, Vol. 31 No. 8, pp. 411-423.

Virgillito, D., Catalfo, P. and Ledda, C. (2025), "Wearables in healthcare organizations: implications for occupational health, organizational performance, and economic outcomes", *Healthcare*, Vol. 13 No. 18, pp. 2227-9032.

Wang, T., Duong, T.D. and Chen, C.C. (2016), "Intention to disclose personal information via mobile applications: a privacy calculus perspective", *International Journal of Information Management*, Vol. 36 No. 4, pp. 531-542.

Wang, Y., Asaad, Y. and Filieri, R. (2020), "What makes hosts trust airbnb? Antecedents of hosts' trust toward airbnb and its impact on continuance intention", *Journal of Travel Research*, Vol. 59 No. 4, pp. 686-703.

Wang, Y., Kung, L. and Byrd, T.A. (2018), "Big data analytics: understanding its capabilities and potential benefits for healthcare organizations", *Technological Forecasting and Social Change*, Vol. 126, pp. 3-13.

Wirth, J. (2018), "Dependent variables in the privacy-related field: a descriptive literature review".

Wright, R. and Keith, L. (2014), "Wearable technology: If the tech fits, wear it", *Journal of Electronic Resources in Medical Libraries*, Vol. 11 No. 4, pp. 204-216.

Xu, H. (2007), "The effects of self-construal and perceived control on privacy concerns".

Xu, H., Dinev, T., Smith, H.J. and Hart, P. (2008), "Examining the formation of individual's privacy concerns: toward an integrative view".

Xu, H., Dinev, T., Smith, J. and Hart, P. (2011), "Information privacy concerns: Linking individual perceptions with institutional privacy assurances", *Journal of the Association for Information Systems*, Vol. 12 No. 12, p. 1.

Yang, H., Yu, J., Zo, H. and Choi, M. (2016), "User acceptance of wearable devices: an extended perspective of perceived value", *Telematics and Informatics*, Vol. 33 No. 2, pp. 256-269.

Yun, H., Lee, G. and Kim, D.J. (2019), "A chronological review of empirical research on personal information privacy concerns: an analysis of contexts and research constructs", *Information and Management*, Vol. 56 No. 4, pp. 570-601.

Zhang, B., Chen, C., Lee, I., Lee, K. and Ong, K.L. (2025), "A survey on security and privacy issues in wearable health monitoring devices", *Computers and Security*, Vol. 155, p. 104453.

Zhang, Y. and Rau, P.L.P. (2015), "Playing with multiple wearable devices: exploring the influence of display, motion and gender", *Computers in Human Behavior*, Vol. 50, pp. 148-158.

Zhang, Y., Wan, G., Huang, L. and Yao, Q. (2015), "Study on the impact of perceived network externalities on consumers' new product purchase intention", *Journal of Service Science and Management*, Vol. 8 No. 1, p. 99.

Further reading

Smith, H.J., Dinev, T. and Xu, H. (2011), "Information privacy research: an interdisciplinary review", *MIS Quarterly*, Vol. 35 No. 4, pp. 989-1015.

Appendix. Questionnaire items.

All items were measured using a five-point Likert scale (1 = strongly disagree, 5 = strongly agree).

Privacy Concerns (Dinev and Hart, 2006):

- I am concerned that wearable devices will collect too much data about me.
- I am concerned that unauthorized individuals could access the personal data I provide to wearable devices.
- I am concerned that my personal data may be used for purposes I am not aware of.
- I am concerned that my personal data stored in wearable device databases will not be adequately protected.

Privacy Control (Xu, 2007):

- I believe that I have control over who can access the data I provide to wearable devices.
- I believe that I have control over the personal data collected by wearable devices.
- I believe that I have control over how my personal data is used by wearable devices.
- I believe that I can control the personal data I provide to wearable devices.

Perceived Effectiveness of Privacy Policy (Xu *et al*., 2008):

- I believe that my organization's privacy policy reflects respect for individuals' privacy when using wearable devices.
- Considering my organization's privacy policy, I believe that the personal data I provide will remain private and confidential.
- I am confident that my organization's privacy policy ensures that my privacy is protected when using wearable devices.

Perceived Risks (Yang *et al*., 2016; Verdegem and De Marez, 2011; Malhotra *et al*., 2004; Jarvenpaa *et al*., 1999; Stone and Grønhaug, 1993)

Privacy Risk:

- It would be risky to disclose my personal data to wearable devices.
- There would be high uncertainty associated with providing my personal data when using wearable devices.

- There would be a high likelihood of privacy loss when providing personal data to wearable devices.
- Providing information to wearable devices would involve many unexpected problems.

Performance Risk:

- I am concerned whether wearable devices will provide the expected benefits (e.g. functionality).
- Wearable devices may lead to privacy violations.
- Wearable devices may not function satisfactorily (e.g. measurement accuracy, quality issues).

Social Risk:

- My colleagues would look at me differently if they saw me using wearable devices.
- I would feel uncomfortable wearing wearable devices.
- People around me might laugh at me if I adopted a wearable device.

Perceived Benefits (Fox *et al.*, 2021; Li *et al.*, 2016; Xu *et al.*, 2011)

Personalized Benefits:

- Providing data to wearable devices may offer personalized services tailored to my activity history.
- Providing data to wearable devices may provide more relevant information based on my preferences and interests.
- Providing data to wearable devices may deliver content that suits my personal preferences.

Work-related Benefits:

- Providing data to wearable devices would improve my ability to manage my work.
- Providing data to wearable devices would improve my access to information.
- Providing data to wearable devices would improve the quality of my work.

Trust (Magni *et al.*, 2021; Gu *et al.*, 2009):

- I feel safe in my workplace.
- I believe that my colleagues are trustworthy.
- I believe that my employer is trustworthy.
- I trust my colleagues if they recommend using wearable devices.
- I trust my employer if they suggest using wearable devices.
- I trust my organization if it encourages the use of wearable devices.

Intention to Use (Li *et al.*, 2019; Pan and Jordan-Marsh, 2010):

- I believe that providing data to wearable devices is a good idea.
- I would be interested in providing data to wearable devices.
- I intend to provide data to wearable devices when given the opportunity in the future.
- I am likely to provide personal data to wearable devices to better meet my needs.

Corresponding author
Maria Vasilidou can be contacted at: mvasilid@pme.duth.gr