Alexander Richter, Patrick Kühtreiber, and Delphine Reinhardt: *On the Impact of Information Provided to Employees on their Intention to Disclose Data Collected by Smart Watches to their Employers.* Proceedings of the 30th European Conference on Information Systems (ECIS), 2022.

# ON THE IMPACT OF INFORMATION PROVIDED TO EMPLOYEES ON THEIR INTENTION TO DISCLOSE DATA COLLECTED BY SMART WATCHES TO THEIR EMPLOYERS

*Research Paper*

Alexander Richter, Computer Security and Privacy, Institute of Computer Science, University of Göttingen, Germany, richter@cs.uni-goettingen.de

Patrick Kühtreiber, Computer Security and Privacy, Institute of Computer Science and Campus Institute Data Science, University of Göttingen, Germany, kuehtreiber@cs.uni-goettingen.de

Delphine Reinhardt, Computer Security and Privacy, Institute of Computer Science and Campus Institute Data Science, University of Göttingen, Germany, reinhardt@cs.uni-goettingen.de

## Abstract

*Companies are increasingly equipping employees with smart watches to improve employees' performance, health, or safety. Thus employers can collect sensitive employees' data using smart watches, including, e.g., employees' health and emotions. This paper investigates the effects of employers' provided information on the employees' intention to share information like activity, health, and location when equipped with a smart watch, considering the privacy calculus. To this end, we have conducted a scenario-based online survey with 1,214 participants in which they have to imagine being equipped with a smart watch by their employer. The scenario was changed in a post-test by increasing employers' provided information to measure the impact of this change on the participants' decisions. Our results indicate that the more information employers provide, the less the participants are willing to disclose data. Therefore, employees who obtain transparent information tend to weigh risks significantly higher in the associated cost-benefit analysis.*

*Keywords: Privacy, Smart watches, Employees' attitudes, Provided information*

## 1 Introduction

An increasing number of employers are relying on information technologies to monitor their employees (Collins and Marassi, 2021). As a result, they gather data about their employees from different sources to investigate, e.g., attitudes and monitor the performance (Bhave et al., 2020). Among existing systems, we especially focus on smart watches, which are increasingly integrated into processes to support employees in carrying out their work and increase their productivity (Maltseva, 2020). Employees can benefit from smart watches due to their unique characteristics (Aehnelt and Urban, 2014). These include their permanent availability, ease of use, and attachment to the body, which allows almost hands-free ubiquitous access to information, and thus support for mobile processes (Zenker and Hobert, 2019; Ziegler et al., 2015). Moreover, smart watch embedded sensors can promote employees' health (Lingg et al., 2014) or increase occupational safety (Choi et al., 2017). However, smart watches can determine and track wearers' location (Filippoupolitis et al., 2017) or even recognize current activity based on sensor data (Davoudi et al., 2019; Mekruksavanich et al., 2018). Therefore, employers can use smart watch data to check

whether the employees are at their workplace (Sen et al., 2016), track their smoking behavior (Shoaib et al., 2015), or infer the employees' general health (Prawiro et al., 2019) and emotions (Tirabeni, 2020). Furthermore, smart watches are usually continuously worn, while a smartphone and other information systems are not (Chen et al., 2014). As a result, this generates a continuous data flow, which employees may interpret as a privacy invasion by their employers. This may lead to stress and reduced productivity (Meyers, 2003; Tomczak et al., 2018), especially when employees consider privacy risks. Thus, it could be recommended that companies consider employees' willingness to adopt these devices, which collect data about them. In addition to the data collection in itself, employer-provided information to employees about the future integration of smart watches can impact their acceptance. For employees to make an informed decision, an employer should provide them with all necessary information before deploying such devices. Thus, *employer-provided information* should include details about data collection, usage, and storage. However, privacy policies have been shown to be challenging to understand (Princi and Krämer, 2019; Ur et al., 2012) and often ignored (McDonald and Cranor, 2008). Additionally, employees may underestimate the privacy risks resulting from the smart watches, which leads to a lack of awareness and knowledge (Princi and Krämer, 2019). Nevertheless, providing this information could further lead to potential conflicts, as employers need to seek employees' consent in advance before they can legally collect and analyze employees' data (Bhave et al., 2020). This, in turn, usually requires employees' acceptance to use such devices, which benefits both employers and employees (Jacobs et al., 2019), thus highlighting the importance of the employees' opinions and decisions. Even if collective agreements between employers and employees are legally possible to bypass individual employees' decision, the employees' consent is requested when pilot studies about the possible integration of smart watches are conducted. By conducting these studies, companies can identify possible negative effects of smart watches on employees and/or their working conditions and mitigate them before their deployment. Such studies are important, as some works councils expect the submission of such studies that show the absence of negative effects before negotiating works agreements (Hobert and Schumann, 2018). Nevertheless, when considering the implementation of smart watches with various benefits and risks, the importance of treating employees fairly is beyond question. However, even when recommendations for employers in the light of employees' monitoring were made (Tomczak et al., 2018; Weston, 2015), none stated anything about the amount and quality of information employees should receive. Therefore, within the scope of this paper, our objective is to investigate how the amount of information regarding the benefits and risks of smart watches affect employees' decision to share data with their employers, resulting in the following *Research Questions (RQ)*:

**RQ1** Does more extensive information provided to the employees increase their willingness to disclose private information to their employer?

**RQ2** How does the provision of more extensive information influence the relationship between perceived risk, benefits, and the intention to disclose information?

We assume that the more information is provided by employers regarding benefits and risks arising from smart watches, the more employees are willing to share the collected data with their employers. To answer these research questions, we develop a research model based on the privacy calculus theory that, in addition to the impacts of perceived benefits and risks on employees' disclosure intention, also includes trust and legislation protection. The research model has been evaluated using a study with 1,214 full-time employees from Germany. The key insights are as follows: (1) We find that employees distinguish between the different data types. They are less likely to share health data with their employers than activity or location data. (2) We find that information about benefits and risks of smart watches provided to employees affect the employees' willingness to disclose information, especially when more obvious risks-related aspects regarding the implementation and usage of smart watch data are provided, which leads to a decreasing willingness to disclose data.

The remainder of our paper is structured as follows: In Sec. 2, we discuss the theoretical background, before presenting our research model in Sec. 3. We detail our methodology in Sec. 4 applied in our

scenario-based online study. In Sec. 5, we present the respective results and discuss our findings in Sec. 6, before making concluding remarks in Sec. 7.

## 2 Theoretical foundation and related research

**Privacy calculus:** Several models were used to explain new technology acceptance, like the *Technologie Acceptance Model (TAM)* (Huang and Kao, 2015; Kim and Shin, 2015). However, these neither consider the impact of user privacy attitudes (Princi and Krämer, 2019) nor the related impact of information disclosure on the intention to use new technologies. This gap has been closed by different authors, who extended the established models by components related to privacy aspects (Weinhard et al., 2017). Privacy is described by Westin (1967) as "the claim of individuals [. . . ] to determine for themselves when, how, and to what extend information about them is communicated to others." In other words, it is the individual's decision to reveal or hide private information. In order to explain the behavior behind such decision, several models, such as the *Communication Privacy Management (CPM)* or the *privacy calculus model*, were developed. Both share similarities regarding the trade-off between costs and benefits as well as risks associated with disclosure (Anderson and Agarwal, 2011). However, whereas the trade-off in CPM theory is associated with disclosure in interpersonal situations (Petronio, 2002), the trade-off in the privacy calculus model is related to the disclosure of information to an organization (Anderson and Agarwal, 2011). The privacy calculus was initially developed as the "calculus of behavior" by Laufer and Wolfe (1977) and considered the underlying mental process of people's disclosure decisions regarding future consequences of their behavioral reactions. In other words, before people tend to disclose personal information, they often compare the social benefits with the negative consequences of such a disclosure. Later, Culnan and Armstrong (1999) applied the model in information systems. Since then, the privacy calculus theory has become widely used in diverse contexts to explain privacy-related decision behaviors regarding personal information disclosure (Dinev and Hart, 2006; H. Li et al., 2016). The privacy calculus is a trade-off, in which an individual weighs the costs against the benefits. Concerning the context of privacy, such costs are often associated with certain risks, which can arise from information disclosure, and may emerge due to the loss of control of personal information, identity theft, or data sharing with third parties (Dinev and Hart, 2006). In contrast, potential benefits are monetary rewards, personalization (Smith et al., 2011), or locatability (Xu et al., 2009). Studies that apply the privacy calculus to users of smart devices, e.g., smart watches, show that the perceived intrinsic value of these devices outweigh the users' privacy concerns (Wieneke et al., 2016). Perceived surveillance, however, increased the privacy concerns (Cho et al., 2018), which shows that transparency of data usage is paramount. Privacy calculus has also been conceptualized (Kalckreuth and Feufel, 2021) and confirmed (Jernejcic and El-Gayar, 2021; H. Li et al., 2016) as the basis for decision making in the context of wearables for, e.g., health purposes. H. Li et al. (2016), for example, examined individuals' adoption of wearable health devices and found, e.g., that health information sensitivity increases the perceived privacy risk, while legislative protection has a decreasing effect. In the context of mobile device location disclosure, a model based on the privacy calculus showed that monetary incentives lead to more willingness to disclose data, but users remain unaware of the associated privacy risks (Naous et al., 2019). The privacy calculus model has also been used in the context of employees' privacy (Chatterjee et al., 2021) and to investigate employees' acceptance of a smart emergency detection system based on employees' tracking (Princi and Krämer, 2019). Apart from using the privacy calculus, other authors have already considered privacy in their studies. Regarding the workplace setting, Schall Jr et al. (2018) found in a study about wearable sensors used for occupational safety and health that privacy concerns prevent adopting such devices and that a better understanding of privacy concerns is needed to address these concerns.

**Provided information:** The importance of treating and informing employees fairly when electronic monitoring is planned is undoubtedly beyond question. Previous research on electronic performance monitoring has already made some recommendations or rules for employers when considering the de-

ployment of electronic performance monitoring to reduce potential negative effects while increasing the positive ones (Tomczak et al., 2018; Weston, 2015). According to the rules, employees should be informed about data collected or accessed and their options to access and correct that information (Weston, 2015). In comparison, the recommendations include that employers should only monitor work-related behavior in a manner that is transparent for employees. Moreover, obtained insights should be used only for learning and not for preventing unwanted employee behavior (Tomczak et al., 2018). Those recommendations and rules already indicate the importance of treating employees fairly. After all, there is no doubt that the fair treatment exercised by employers would lead to greater employee understanding and acceptance of monitoring devices. Nevertheless, the question arises as to how that information needs to be presented by the employer to inform employees properly. Accordingly, we have to find out the amount and kind of information that an employer should provide to the employees in a fair and useful way. The employees should be able to understand the potential benefits such devices can provide, but also which risks are conceivable, to be then able to weigh risks and benefits. This, in turn, can lead to an increase in employees' willingness to share their personal data with their employers. Especially when considering how information regarding employers' privacy notices are presented or formulated for the employees, the question arises how these privacy notices influence employees' willingness to disclose personal data. This is not only to treat employees fairly by providing them with transparent information but also because privacy notices with less privacy protection lead users to disclose fewer data (Adjerid et al., 2013). Because even when objective risks from disclosure stay constant, the users' willingness to disclose data online increases when the notices are framed in a privacy-increasing way and vice versa (Adjerid et al., 2013). Thus, e.g., privacy notices could be deliberately framed in a more protective way to increase users' willingness to disclose more personal data than is justified by the protection of privacy (Adjerid et al., 2013), which should not be in the employers' intent.

**Summary:** Various models were developed to explain users' acceptance of devices or their intention to disclose private data. Especially regarding privacy, the privacy calculus, in which the trade-off between benefits and risks is analyzed, was used to explain that intention. Various authors changed the constructs of the calculus to explain their impact. Thereby, the calculus was also applied in the corporate context and extended by different constructs. Thus, in what follows, we decide to use the privacy calculus as the underlying theory and reject models that focus solely on acceptance because employees usually have less power to decide whether to accept or reject such devices unless quitting their jobs. Therefore, the introduction of such devices may lead to private information disclosure that would involve a privacy calculus, in which employees may face a trade-off between perceived benefits and privacy risks (H. Li et al., 2016). Thus, the privacy calculus theory seems to be more suitable to understand employees' intention to disclose private information to the employer when they are expected to use smart watches. However, insights are missing about the impact of information provided on employees' decision to share data with their employer before implementing smart watches based on the perceived privacy risks and benefits.

## 3 Research model and hypotheses

To answer the research questions from Sec. 1, we propose a research model (see. Fig. 1) and describe our research model's used constructs and corresponding hypotheses in more detail in the following for each construct.

**Perceived benefits:** The perception of benefits is necessary to overcome the perception of potential privacy risks to ultimately disclose personal data. Whether employees outweigh benefits over privacy risks depends on several personal factors, which may arise from an employee's prior knowledge or experience. The acceptance models suggest that the perceived usefulness of new technology leads to a positive impact on the acceptance of new technologies in an organization. This perceived benefit relates to

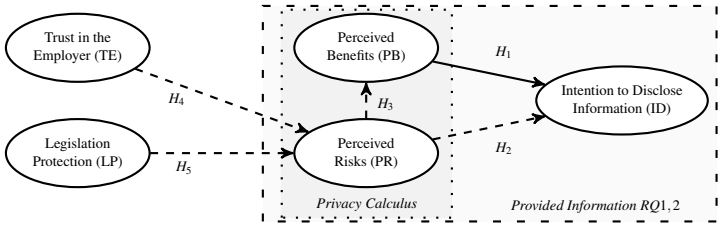



*Figure 1. Research model*

the enhancement of the job performance (Choi et al., 2017) or reflects the benefits that a user gains when utilizing such systems (J. Li et al., 2019). By using wearable devices, directly connected to an employee, further potential benefits (e.g., improving employees' health or occupational safety) may arise, which an employee must first perceive as a benefit and subsequently include it in her/his privacy calculus. For that, smart watches offer a variety of benefits at the workplace. For example, smart watches maximize employees' efficiency and productivity (Khakurel, Melkas, et al., 2018; Weston, 2015) achieved through faster access to helpful information directly on the smart watch. Another example is the productivity enhancement when determining employees' locations and providing them with helpful information to improve their routes in a warehouse (Tirabeni, 2020). Apart from such benefits, smart watches could be used for various applications within workplace environments. This includes the stimulation of individual physical activity encouraged by corporate wellness programs (Maltseva, 2020; Tirabeni, 2020), the detection of work-related stress and fatigue (Maltseva, 2020; Mettler and Wulf, 2019), or the improvement of employees' safety in case of hazardous situations using warning signals (Choi et al., 2017; Maltseva, 2020). Considering the previous findings, we expect, therefore, the following:

**H1** Perceived benefits are positively associated with the intention to disclose *activity/health/location* information.

**Perceived risks:** The disclosure of personal information gathered by a smart watch at work can result in the perception of privacy risks. Apart from identity theft or financial losses in a private scenario, the privacy risks in a workplace context may result in other negative consequences. The fact that wearable devices are in the position to violate privacy when generating data, such as employees' vital information is already identified in different studies (Khakurel, Pöysä, et al., 2016; Mettler and Wulf, 2019). Thus, smart watches enable employers to collect a vast amount of extremely detailed and highly personalized information about their employees, which employers could use, e.g., to achieve organizational goals such as reducing the workforce (Mettler and Wulf, 2019). Wearable devices employed in that manner may harm employees' privacy and represent a new level in monitoring and control. Likewise, Tirabeni (2020) mentioned that employers' control had been slowly shifted from only monitoring employees' work to also monitoring their bodies, which allows a different level of workplace monitoring. In that way, the constant monitoring through wearable devices provides employers a deep understanding of all employees' data (Tirabeni, 2020). This may lead to an imbalance between employers and employees. Apart from previously mentioned smart watch benefits regarding the workforce's well-being or occupational safety, the introducing paragraphs of this section also indicated the dark side of smart watches. Especially when considering the required health or activity data for well-being or location data for occupational safety, which are undoubtedly high sensitive personal data. Employees initially have few privacy concerns about using technology to count their daily number of steps (Barata and Cunha, 2019), for example, as they often do not understand what the consequences of such disclosures can be (Gorm and Shklovski, 2016). However, once employees are aware of potential risks, this negatively impacts employees' perceptions of the smart watches' perceived value and hinders the use, even when employees understand their potential benefits (Choi et al., 2017). Additionally, privacy concerns may arise because the personal data may end up in the wrong hands, the providers or external parties may gain access to the data (Häikiö et al., 2020).

Considering these insights from the literature, we formulate the following hypotheses:

**H2** Perceived risks are negatively associated with the intention to disclose *activity/health/location* information.

**H3** Perceived risks negatively influence employees' perceived benefits.

**Trust in the employer:** Apart from the perceived benefits and privacy risks, perception of trust as "the confidence that the other party to an exchange will not exploit one's vulnerabilities" (Korczynski, 2000) plays an essential role in the interaction between two parties. Especially when considering information asymmetries between two parties, trust is crucial in mitigating risk perceptions when one party has less information than the other and is thus unable to accurately determine if they are treated fairly because of their lack of knowledge (Anderson and Agarwal, 2011). Prior research in the light of self-disclosure to an organization indicates that individuals are more willing to disclose personal information when having a high degree of trust and are aware that the organization applies fair methods for managing such information (Anderson and Agarwal, 2011). Likewise, research in the context of self-disclosure online suggests that users' trust in a company affects their willingness to disclose more information online (Bol et al., 2018; Fletcher and Park, 2017). In a work-related context, trust in the employer is also crucial in employees' readiness to accept being monitored by various sensors (Princi and Krämer, 2019). This is because of the employer-employee relationship, which is often characterized by an imbalance in decision-making power or information control of the parties (Princi and Krämer, 2019). Hence employees are often limited in their actions when employers plan to introduce employee monitoring. However, employees' trust in the employer can be damaged with intense employee monitoring, which negatively impacts employee productivity (Allen et al., 2007). Besides, trust is also negatively affected by the perceived amount of data tracking in the workplace (Change et al., 2017). This can also be seen when data collected is used to punish them (George, 1996). Despite that, Princi and Krämer (2019) indicates that employees' trust in their employer did not mitigate employees' perceived privacy risks when introducing a smart monitoring system as employees might expect more severe consequences due to the personal data gathering. However, they also postulate that trust in the employer is important as employees would accept a privacy-invading tracking system as long as they trust their employer. In addition, the literature suggests that trust is a crucial construct that facilitates the overcoming of perceived risks concerning uncertainty and fear (McKnight and Chervany, 2001; Princi and Krämer, 2019). Along with the previous research and the insights regarding workplaces, we expect the following:

**H4** Trust in the employer is negatively associated with perceived risks.

**Legislation protection:** Laws regulate various social conditions in different areas, such as business life, labor market, and data protection. However, regulations always follow market requirements, as governments, e.g., seek to protect people's private data against misuse by companies or fraud. However, the organizational protection of individuals' privacy seems to be already a driver for potential consumer attraction (J. Li et al., 2019). Thus, companies use various strategies, e.g., privacy policies, to reduce consumers' privacy concerns, as consumers ordinarily tend to oppose improper processing of personal data, and companies are aware of this (Dinev, Xu, et al., 2013; H. Li et al., 2016). Nevertheless, a certain skepticism existed with regard to the effectiveness of industrial self-regulation to ensure consumer privacy, resulting in calls stronger legislation to curb the potential company information misuse (Dinev, Xu, et al., 2013; Smith et al., 2011). Certainly influenced by this, the EU has enhanced the legislation to this end in recent years, which confirms the importance of consumer protection from companies' improper processing of personal information. This also affects employees' data gathered in companies for diverse purposes. The *General Data Protection Regulation (GDPR)*, however, does not regulate the protection of employee data in detail, which is left to the responsibility of the member states (Art. 88 GDPR). Therefore, the German government, e.g., has reissued the *Bundesdatenschutzgesetz (BDSG)* to supplement, concretize, and specify

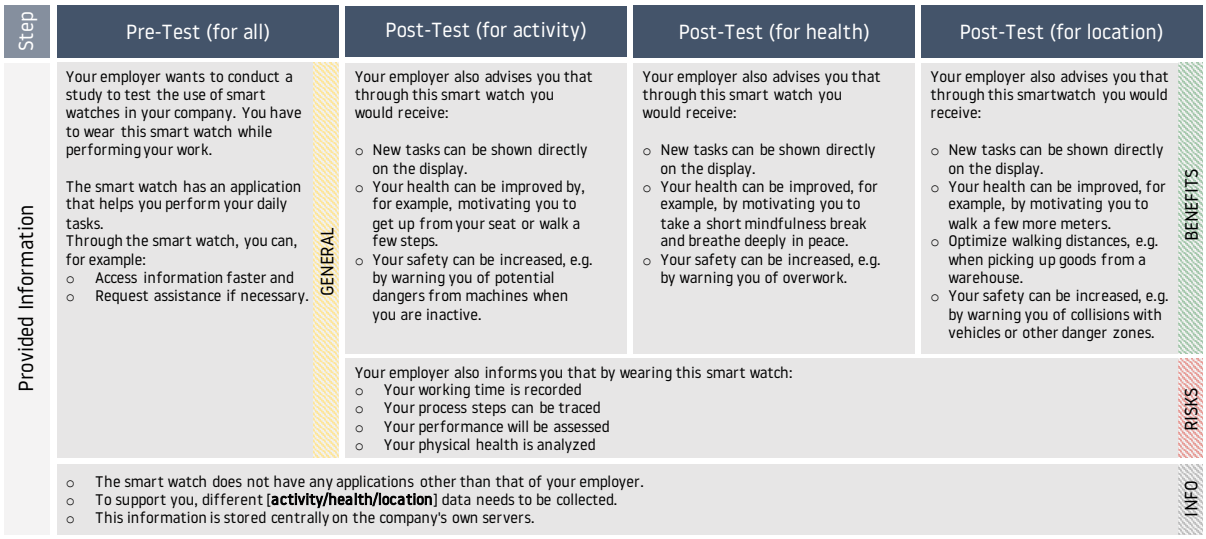



*Figure 2. Overview of provided information in the given scenario*

these requirements. Besides, the *Betriebsverfassungsgesetz (BetrVG)* is essential for German companies. Gathering employees' data, in particular, includes employees' names, addresses, or phone numbers. However, especially the deployment of smart watches with various built-in sensors that employees have to wear when carrying out the work makes it possible to gather more sensitive data about employees. This enables employers to obtain information about employees' state of health, for instance. Indeed, collective agreements are possible (§ 26 Par. 4 BDSG) to bypass the individual employees' consent and are certainly mainly used in practice. In addition, the works council must be involved when the deployment and use of technical devices designed to monitor the employees' behavior or performance are considered (§ 87 Par. 1 No. 6 BetrVG). However, such regulations seem to provide a certain degree of privacy protection, which could affect employees' behavior to disclose personal information, since employees possibly trust such regulations due to their belief that governments can punish undesired behavior. Previous studies on privacy could already demonstrate a negative effect on the perceived privacy risks by legislation protection (Dinev, Xu, et al., 2013; H. Li et al., 2016; Xu et al., 2009). Xu et al. (2009) examined the negative impact of privacy-related intervention in governmental regulations in location-based services. Likewise, Dinev, Xu, et al. (2013) demonstrated that regulatory expectations could effectively reduce individuals' perceived risk as a predictor of perceived privacy. Further, H. Li et al. (2016) showed that the legislative protection negatively affects individuals' perceived privacy risk regarding the adoption of healthcare wearable devices. Considering the above and the results of previous studies, we assume that:

**H5** Legislation is negatively associated with perceived risks.

# 4 Methodology

In the following, we explain our research methodology by providing details about our survey design, survey distribution, and analyses we conducted. Moreover, we also acknowledge survey limitations.

**Survey design:** To test our hypotheses, we have conducted a user study based on an online questionnaire in German containing four parts. First, questions about demographics (gender and age) to comply with the survey's quotas. Second, questions regarding trust in the employer in handling their data and their belief in the legislation protection to prevent employer's misuse of personal data. Third, a pre- and post-test with questions regarding perceived benefits, risks, and intention to disclose private information. In more detail, our participants have to imagine themselves in a scenario in which their employer provides them with

| Constructs | Measurement items | Source |
|---|---|---|
| Intention to Disclosure (ID) | ID1: I am likely to disclose my *activity, health, location* information by using a smart watch<br>ID2: I am willing to disclose my *activity, health, location* information by using a smart watch<br>ID3: I am definitely willing to share my *activity, health, location* captured by the smart watch with my employer | Bansal et al., 2010; T. Wang et al., 2016; Xu et al., 2009 |
| Perceived Benefits (PB) | PB1: I believe that using a smart watch would improve my *health* in doing my job<br>PB2: I believe that using a smart watch would improve my *safety* in doing my job<br>PB3: I believe that using a smart watch would increases my *productivity* in doing my job | Choi et al., 2017; Kim and Shin, 2015; H. Li et al., 2016 |
| Perceived Risks (PR) | PR1: I believe that it would be risky to disclose my personal information to my employer<br>PR2: I believe that there would be high potential for loss associated with disclosing my personal information to my employer<br>PR3: I believe that there would be too much uncertainty associated with giving my personal information to my employer | H. Li et al., 2016 |
| Legislative Protection (LP) | LP1: I believe that the law should protect me from the misuse of my personal data by my employer<br>LP2: I believe that the law should govern and interpret the practice of how my employer collect, use, and protect my private information<br>LP3: I believe that the law should be able to address violation of the information I provided to my employer | Dinev, Xu, et al., 2013 |
| Trust in the Employer (TE) | TE1: I believe that my employer handle my personal information confidentially<br>TE2: I believe that my employer handle my personal information correctly<br>TE3: I believe that my employer are always honest to me about how they use my personal information<br>TE4: I believe that my employer protect my personal information I share with them | Bol et al., 2018; Princi and Krämer, 2019 |

*Table 1. Constructs and Measurement items*

information about the upcoming smart watch deployment. The pre- and post-test vary in the information provided. The pre-test provides general information, such as (1) general conditions for the smart watch integration, (2) data collection and storage, and (3) explanatory benefits that result from the integration. The post-test, however, lists (1) potential smart watch benefits for the enterprise applications in addition to the data that has to be collected and (2) possible smart watch use cases where potential risks are more obvious. The information provided in the scenarios are summarized in Fig. 2 , while Sec. 4 provides an overview of the constructs' used items. For all these constructs items, participants were able to select each from a 5-point Likert scale that ranges from "strongly disagree" to "strongly agree". The last part contains several questions about participants' demographics, such as their working sector, which kind of function they hold, and how long they are working for their company. Our questionnaire follows a 3x2-mixed design, in which our participants were split into activity, health, and location data. Hence, we asked them about their intention to share just these data respectively (between-subject-factor) with their employer by providing the participants with different information in two subsequent steps regarding the previously described smart watch scenario (within-subject-factor) presented in Fig. 2. The change in the provided information can be seen as an intervention of a subject's decision-making. Hence, it surrounds the three constructs that we assumed influence employees' decision-making represented by the dashed line in Fig. 1.

**Survey distribution:** Our online study was reviewed and approved by our university's ethics committee and data protection officer and complied with ethical guidelines and legal requirements. The survey participants were invited by an ISO 26362 certified survey panel and monetarily rewarded. All 1,214 participants were full-time employees working different sectors in Germany aged 18 years and above. Both distributions in terms of age and gender are representative for the German population (Statistisches Bundesamt (Destatis), 2021). Note that our participants were evenly distributed across three separate questionnaires considering different data types, i.e., activity (395 participants), health (406), or location data (413). Sec. 4 lists the demographics and characteristics of our sample.

| Levels | | Count | Percentage |
|---|---|---|---|
| Gender | Male | 590 | 48.6% |
| | Female | 624 | 51.4% |
| Age | 18–24 | 179 | 14.7% |
| | 25–34 | 262 | 21.6% |
| | 35–44 | 299 | 24.6% |
| | 45–54 | 361 | 29.7% |
| | 55–67 | 113 | 9.3% |

*Table 2. Sample characteristics (N= 1,214).*

| Construct | mean | sd | $\alpha$ | $\omega$ | AVE | TE | LP | PB | PR | ID |
|---|---|---|---|---|---|---|---|---|---|---|
| *Recommendation* | - | - | *>.70* | *>.70* | *>.50* | - | - | - | - | - |
| Trust in the Employer (TE) | 4.37 | 0.72 | 0.93 | 0.93 | 0.78 | **0.881** | | | | |
| Legislation Protection (LP) | 3.96 | 0.77 | 0.73 | 0.75 | 0.50 | 0.312 | **0.706** | | | |
| Perceived Benefits (PB) | 2.57 | 1.09 | 0.88 | 0.88 | 0.70 | 0.030 | 0.076 | **0.838** | | |
| Perceived Risks (PR) | 2.98 | 1.11 | 0.92 | 0.92 | 0.79 | 0.141 | 0.045 | 0.057 | **0.889** | |
| Intention to Disclosure (ID) | 2.82 | 1.36 | 0.97 | 0.97 | 0.92 | 0.067 | 0.062 | 0.479 | 0.246 | **0.957** |

*Note: Alpha, internal consistency (Cronbach's alpha); Omega, composite reliability; AVE: Average Variance Extracted; Diagonal values in boldface are the square roots of the AVEs;*

*Table 3. Descriptive statistics, reliability and correlations of measured constructs*

**Data analyses:** A *Confirmatory Factor Analysis (CFA)* was used on the collected data to perform a reliability and validity test of the measurements and a *Structural Equation Modeling (SEM)* was conducted to analyze the strength and directions along the paths between the constructs in order to analyze and test our hypotheses using a significance level of 5%. Both were conducted with a maximum likelihood estimation method with robust standard errors and a Satorra-Bentler scaled test statistic (Kline, 2016, p. 77), as the normal distribution assumption was violated for some items. For all models, gender and age were controlled. Sec. 4 summarizes used items for each measurement model construct. For examining the internal reliability, and convergent and discriminant validity, we calculated Cronbach's alpha, composite reliability (Raykov's $\omega$), and *Average Variance Extracted (AVE)*, which are widely used measurements (Fornell and Larcker, 1981). Tab. 3 summarizes recommended (according to (Hair et al., 2014; Hu and Bentler, 1999)) and determined values for each construct in the measurement model. As the participants are separated into three distinct groups regarding data types (i.e., activity, health, location), we test the groups for strict measurement invariance (Kline, 2016, p. 399). A strict measurement invariance allows comparisons across groups as latent factors measure the same construct. To test RQ1 and RQ2, we compare the pre- and post-models to indicate changes along the paths.

**Survey limitations:** We acknowledge some survey limitations. First, the collected data relates only to participants located in Germany so that the culture may influence the results. Second, to have a wider range of participants, we did not classify in advance which kind of workplace a participant has to work in to participate. This may have led to the effect that the employees had different perspectives due to their workplace situation. Finally, we asked participants just about their intention to disclose only activity, health, or location data each, which leads us to the point that we are not able to conclude something about their ratio of requested data and hence nothing about their willingness to disclose, e.g., activity rather than health data and vice versa.

# 5 Results

In this Section, we provide the results. We first present the results determined by an SEM on the model itself. We then determine additional measurements regarding the influence of age or gender. Moreover, we

| Fit indices | CFI | TLI | NFI | GFI | AGFI | RMSEA | SRMR |
|---|---|---|---|---|---|---|---|
| Recommendation | $> 0.90$ | $> 0.90$ | $> 0.90$ | $> 0.95$ | $> 0.95$ | $< 0.08$ | $< 0.08$ |
| Measurement | 0.99 | 0.99 | 0.98 | 0.97 | 0.96 | 0.03 | 0.03 |
| Structural | 0.99 | 0.98 | 0.98 | 0.97 | 0.95 | 0.04 | 0.05 |

*Note: CFI, Comparative Fit Index ; TLI, Tucker-Lewis Index; NFI, Normalized Fit Index; GFI, Goodness of Fit Index; AGFI, Adjusted Goodness of Fit Index; RMSEA, Root Mean Square Error of Approximation; SRMR, Standardized Root Mean Square Residual;*

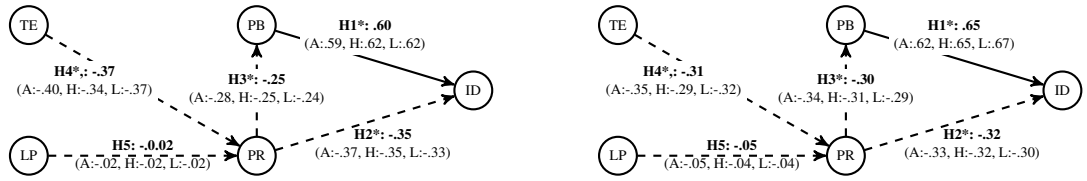
*Table 4. Fit indices of measurement and structural model*

compare employees' intention to disclose data to their employer based on the different data types (i.e., activity, health, location). At last, we compare the changes after the post-test.

**Measurement model:** The measurements displayed in Tab. 3 indicate acceptable reliability for this study as Cronbach's alpha, composite reliability, and AVE are mainly above their recommended thresholds. Only the construct *"Legislation Protection"* has a low AVE value. However, as the value for composite reliability is higher than 0.6, we can assume that construct's convergent validity is still adequate (Huang, Y. Wang, et al., 2013). To evaluate the discriminant validity, the square root of the AVE of a construct and the correlation coefficients to this construct can be compared. For all constructs, the AVE square roots were greater than the correlation coefficients shown in Tab. 3, indicating acceptable discriminant validity (Bock et al., 2005; Fornell and Larcker, 1981). In addition, the CFA fit indices for the measurement model showed acceptable results compared to minimum values recommended in prior studies (see Tab. 4) (Hair et al., 2014; Hu and Bentler, 1999).

**Structural model:** The SEM results presented in Tab. 4 indicate also acceptable model fit indices based on recommended thresholds (Hu and Bentler, 1999). The SEM revealed that for all proposed paths, except for path LP $\rightarrow$ PR (**H5**, $\beta = -0.02$, $p = 0.72$), the standard coefficients $\beta$ were significant. Trust in the employer reduces the perceived risks (**H4**, $\beta = -0.37$). As expected, perceived risks mitigate the perceived benefits (**H3**, $\beta = -0.23$) and intention to disclose private data (**H2**, $\beta = -0.37$), while perceived benefits increase the intention to disclose private data (**H1**, $\beta = 0.56$).

**Measured impacts:** The characteristics of the descriptive values for the main constructs (see Tab. 3) summarized as means revealed high trust in the employer over all participants ($M = 4.37$, $SD = 0.72$). Neither gender nor age have a significant influence on the results. The results for the construct legislation protection are also quite high and do not depend on age or gender ($M = 3.96$, $SD = 0.77$). Considering in the following only the constructs which were asked after the first general provided information. For the construct perceived benefits, the results reveal lower mid mean values ($M = 2.57$, $SD = 1.09$). This perception is not significantly affected by gender but by age ($p < 0.05$, Kruskal-Wallis test). However, this significance results solely from the comparison of the younger with the older age categories. Slightly higher results are obtained for perceived risks ($M = 2.98$, $SD = 1.11$). However, no significant differences between ages or gender can be observed. Finally, we look at the remaining construct of the intention to disclose private data with the employer after providing general information. The data indicate a medium participants' willingness to do so ($M = 2.82$, $SD = 1.36$). Influence of gender and age, however, are not significant. Apart from this, significant differences in the participants' willingness to disclose data to the employer extend within the data types. The data indicate that the participants who were confronted with questions regarding health data achieved significantly lower values ($M_a = 2.95$, $sd_a = 1.28$, $M_h = 2.63$, $SD_h = 1.37$, $M_l = 2.88$, $SD_l = 1.39$, $p < 0.05$, Kruskal-Wallis test). In more detail, a pairwise comparison (Bonferroni corrected) reveals that there is a significant mean difference in their willingness to disclose health related data compared to activity ($M_\Delta = -0.33$) or location ($M_\Delta = -0.25$) data. Our post-test results show slightly different values in the descriptive values. After the intervention perceived benefits ($M = 2.59$, $SD = 1.16$) increased slightly. Likewise, the values for perceived risks ($M = 3.17$, $SD = 1.17$)




(a) Provided information 1 (b) Provided information 2

*Figure 3. Results along the paths for both provided information conditions with negative (dashed) and positive (solid) effects*

| Hypothesis | H1: PB → ID | H2: PR → PB | H3: PR → ID | H4: TE → PR | H5: LP → PR |
|---|---|---|---|---|---|
| Standardized coefficient (pre) | 0.60* | −0.25* | −0.35* | −0.37* | −0.02 |
| Standardized coefficient (post) | 0.65* | −0.30* | −0.32* | −0.31* | −0.05 |
| Supported | Yes | Yes | Yes | Yes | No |

*Note:* $*p < 0.05$

*Table 5. Summary of the hypothesis tests*

are higher, while being lower for the intention to disclose ($M = 2.51$, $SD = 1.32$). This could be seen as a first indication that there has been a change in the participants' attitudes. Moreover, while perceived risks show no significant correlation with age or gender, a significant correlation between perceived benefits and age ($p < 0.001$, Kruskal-Wallis test) and gender ($p < 0.05$, Mann-Whitney U test) is revealed. Also, age significantly impacts the intention to disclose ($p < 0.05$, Kruskal-Wallis test). Along the paths are also slight changes (see Fig. 3). While the negative effect of trust on perceived risks decreased ($\beta_\Delta + 0.06$) the negative one from legislation protection increased slightly ($\beta_\Delta - 0.03$). Likewise, the negative effect of perceived risks on the intention to disclose decreased ($\beta_\Delta - 0.03$) while it increased on perceived benefits ($\beta_\Delta - 0.05$). In comparison, the positive effect of perceived benefits on intention to disclose increased ($\beta_\Delta + 0.05$).

# 6 Discussion

Our studies' primary goal was to examine the impact of employers' provided information regarding smart watch implementation on their employees' intention to disclose private information to the employer. Based on the privacy calculus, we developed a research model that, in addition to the impacts of perceived benefits and risks on employees' disclosure intention, also includes trust, and legislation protection. The first three were measured twice in a pre- and post-test to get insights into the impact of employers' provided information. In the following, we are discussing our hypotheses, followed by discussing the impact on participants' decisions by the intervention we made on the information provided.

According to H1, that employees' **perceived benefits** lead to a higher intention to disclose private data with the employer, the data confirm that positive association. From this, it becomes apparent that when employees are provided with initially very general information, they already recognize advantages in using smart watches in the workplace. At least, the results show that some participants see some benefit from using it. Thus, our findings are similar to previous studies regarding smart wearable acceptance, in which perceived benefits would increase such acceptance (Choi et al., 2017; H. Li et al., 2016) leading consequently to the disclosure of private data.

Our H2 regarding **perceived risks** and its negative association with employees' intention to disclose private data with the employer is supported. This result is consistent with prior studies (Choi et al., 2017; H. Li et al., 2016). Hence, when employees out-weigh perceived risks about the smart watches over their perceived value, it would hinder its use. This is true even when employees understand their potential

benefits. Regarding H3, the negative association on perceived benefits is also supported. Meaning, first of all, that once an employee perceives privacy risks, these will directly negatively impact perceived benefits. In more detail, when employees are more likely to perceive privacy risks in the provision of smart watches and the associated disclosure of private data in work processes, they are less likely to see benefits in their use. In contrast, employees who perceive fewer privacy risks are more likely to notice the benefits. This shows the interaction between perceived benefits and risks and demonstrates that employees also make a risk-benefit trade-off in situations, where their options for action may be limited by the unbalanced relationship between employers and employees. Similar findings for workplace situations arise in the context of the use of a smart emergency detection system, in which perceived benefits positively impact risks (Princi and Krämer, 2019). It can be concluded that - similar to individuals in private situations - employees in workplace situations are conducting a risk-benefit assessment in terms of the privacy calculus, in which individuals, for instance, have to decide whether or not to disclose personal information to use a particular service.

As suggested in H4, **trust in the employer** is negatively associated with perceived risks. In other words, when an employee perceives the relationship with the employer as trustful, this would lead to fewer perceived risks when using smart watches, even if personal activity, health or location data is transmitted to the employer. Thus, our results are similar to previous studies that consider trust in a website as an important factor in individuals' willingness to disclose private data online (Fletcher and Park, 2017). However, this cannot always be assumed in an employment relationship. This is shown by results of Princi and Krämer (2019), where trust in the employer did not lead to fewer privacy risk perceptions. Thus, our results are not similar to the authors' findings, where trust only affects the system's acceptance. One reason for this may be that employees consider a smart monitoring system, which was part of their study, to be riskier than a smart watch. Another may be that, unlike the previous study, participants in this study may not distinguish trust in the increased safety due to the technology from trust in the employer. Regardless of the difference in these two studies, it should be further investigated which impact trust in the employer has on the deployment of technological devices capable of collecting personal data.

Our assumption in H5, that the belief in the **legislative protection** against unwanted employer behavior would lead to perceiving fewer privacy risks, could not be confirmed. Although a negative association can be surmised, this is not significant. Accordingly, it is more likely to conclude that even if employees believe in protection from employers through legislation, this does not significantly impact the perceived privacy risks of using a smart watch and the associated transfer of private data to the employer. Previous studies have already shown that legislative protection can influence individuals' perceived risks in various areas such as location-based services (Xu et al., 2009) or wearable devices in health care (H. Li et al., 2016). However, our results indicate that this influence is different in the case of smart watches in workplaces combined with the disclosure of private data. This demonstrates that the belief in the legislation protection differs in the private and work contexts, which can have different causes. One could be that employees do not consider personal data disclosure to the employer as voluntary and thus may associate more risks with this disclosure, as these risks are more noticeable than in the private sphere. Another reason could be that due to the direct personal relation to their superiors, employees may feel uncomfortable and monitored.

Considering RQ1, whether more extensive **provided information** would lead to higher employees' willingness to disclose data to the employer can be negated. The results reveal that our participants' intention to disclose private data to their employer decreased after the intervention in the post-test. Therefore, contrary to our expectations, that more detailed information concerning benefits and risks when using smart watches leads to an increased willingness to disclose private data, it instead led to a decrease in employees' willingness to do so. This was not expected, as it can be assumed that employees prefer more detailed information and are subsequently more willing to disclose them in return. One reason may be that our participants are already concerned about the topic as a result of the first basic information. The next questions might have indirectly influenced their decision-making. However, the results for perceived risks show that the participants perceive more risks after our intervention. Besides, within a workplace scenario, employees may weigh privacy risks higher than the benefits, especially because risks, when

they occur, are more noticeable than in the private context. Our RQ2, whether more extensive provided information strengthens the positive and weakens the negative relationship between the existing paths between perceived risk, benefits, and the intention to disclose information, can be partially confirmed. The results presented in Sec. 5 and depicted in Fig. 3 revealed the changes from Fig. 3(a) to Fig. 3(b). The path between perceived benefits and intention to disclose is strengthened, meaning that when employees perceive benefits, their willingness to share such data with the employer is strengthened. In comparison, the negative influence of perceived risks on the willingness to share information is weakened, while it is strengthened on the perceived benefits. As a result, the increased perceived risks have a stronger influence on these perceived benefits than before. Moreover, the data show that even trust in the employer decreases in influence on perceived risks after the additional information provided in the following step. This also indicates that employees give greater weight to their perceived risks after being provided with more information. In general, the data reveal that employees are less willing to share data with employers when provided with more information regarding risks and benefits. Thus, employers should simultaneously provide privacy solutions to mitigate such negative influences.

# 7 Conclusions

This study investigated the impact of employers' provided information on employees' willingness to share private data with their employers, based on the privacy calculus. In more detail, we investigated the extent to which the employee's risk-benefit trade-off takes place and how this is influenced by the information provided. To this end, we used a 3x2 mixed online experiment with 1,214 full-time employees. In the corresponding questionnaire our participants were introduced to a scenario in which their employer would provide them with a smart watch to gather different data types (i.e., activity, health, and location). Initially, these scenarios were rather general and then were extended by explicitly mentioning both benefits and risks. This allowed us to observe the effects between the groups, i.e., activity, health, location, and how this change in information affected employees' decisions in general. Our results indicate that employees' provided information about smart watch benefits and risks negatively affects employees' willingness to disclose information when providing them with more obvious risks-related aspects regarding the implementation and usage of smart watch data. These results can help companies to provide employees with more comprehensive information about the smart watch introduction in their companies. However, providing more information about both benefits and privacy risks side by side is not sufficient. Employers should be aware of this and provide adequate solutions for potential risks simultaneously. In the long term, a generational change in the workforce could lead employees to be more open to smart technologies and data disclosure. They are more familiar with the usage and benefits of smart devices from private use and may weigh up the possible risks differently in a cost-benefit trade-off. Nonetheless, employees could be more aware of the risks that might occur due to the employee-employer relationship and hence likewise be less willing to share data with their employer in the future. However, employers should not use their power over their employees to force them to accept any new technologies with the ability to collect personal data, as voluntary use may increase the effectiveness and satisfaction of the employees. Overall, the study contributes to privacy research in workplace environments to help employers draw the right conclusions and proactively provide transparent information to employees.

## References


Adjerid, I., A. Acquisti, L. Brandimarte, and G. Loewenstein (2013). "Sleights of Privacy: Framing, Disclosures, and the Limits of Transparency." In: *Proc. of the 9th Symposium on Usable Privacy and Security (SOUPS)*. Ed. by L. Bauer, K. Beznosov, and L. F. Cranor, 9:1–9:11.

Aehnelt, M. and B. Urban (2014). "Follow-me: Smartwatch Assistance on the Shop Floor." In: *Proc. of the 1st International Conference on HCI in Business, (HCIB)*.

Allen, M., S. J. Coopman, J. L. Hart, and K. L. Walker (2007). "Workplace Surveillance and Managing Privacy Boundaries." *Management Communication Quarterly* 21 (2), 172–200.

Anderson, C. and R. Agarwal (2011). "The Digitization of Healthcare: Boundary Risks, Emotion, and Consumer Willingness to Disclose Personal Health Information." *Information Systems Research* 22 (3), 469–490.

Bansal, G., F. Zahedi, and D. Gefen (2010). "The Impact of Personal Dispositions on Information Sensitivity, Privacy Concern and Trust in Disclosing Health Information Online." *Decision Support Systems* 49 (2), 138–150.

Barata, J. and P. R. da Cunha (2019). "Safety Is the New Black: The Increasing Role of Wearables in Occupational Health and Safety in Construction." In: *Proc. of the 22nd International Conference on Business Information Systems (BIS)*, pp. 526–537.

Bhave, D., L. Teo, and R. Dalal (2020). "Privacy at Work: A Review and a Research Agenda for a Contested Terrain." *Journal of Management* 46 (1), 127–164.

Bock, G.-W., R. W. Zmud, Y.-G. Kim, and J.-N. Lee (2005). "Behavioral Intention Formation in Knowledge Sharing: Examining the Roles of Extrinsic Motivators, Social-Psychological Forces, and Organizational Climate." *MIS Quarterly* 29 (1), 87–111.

Bol, N., T. Dienlin, S. Kruikemeier, M. Sax, S. C. Boerman, J. Strycharz, N. Helberger, and C. H. De Vreese (2018). "Understanding the Effects of Personalization as a Privacy Calculus: Analyzing Self-Disclosure Across Health, News, and Commerce Contexts." *Journal of Computer-Mediated Communication* 23 (6), 370–388.

Change, S. E., A. Y. Liu, and Y.-T. J. Jang (2017). "Exploring Trust and Information Monitoring for Information Security Management." In: *Proc. of the 10th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI)*, pp. 1–5.

Chatterjee, S., R. Chaudhuri, D. Vrontis, and E. Siachou (2021). "Examining the Dark Side of Human Resource Analytics: An Empirical Investigation Using the Privacy Calculus Approach." *International Journal of Manpower*.

Chen, X., T. Grossman, D. J. Wigdor, and G. Fitzmaurice (2014). "Duet: Exploring Joint Interactions on a Smart Phone and a Smart Watch." In: *Proc. of the 2014 SIGCHI Conference on Human Factors in Computing Systems (SIGCHI)*.

Cho, J. Y., D. Ko, and B. G. Lee (2018). "Strategic Approach to Privacy Calculus of Wearable Device User Regarding Information Disclosure and Continuance Intention." *KSII Transactions on Internet and Information Systems (TIIS)*.

Choi, B., S. Hwang, and S. Lee (2017). "What Drives Construction Workers' Acceptance of Wearable Technologies in the Workplace?: Indoor Localization and Wearable Health Devices for Occupational Safety and Health." *Automation in Construction* 84, 31–41.

Collins, P. M. and S. Marassi (2021). "Is That Lawful?: Data Privacy and Fitness Trackers in the Workplace." *International Journal of Comparative Labour Law* 37 (1), 65–94.

Culnan, M. J. and P. K. Armstrong (1999). "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation." *Organization science* 10 (1), 104–115.

Davoudi, A., A. A. Wanigatunga, M. Kheirkhahan, D. B. Corbett, T. Mendoza, M. Battula, S. Ranka, R. B. Fillingim, T. M. Manini, and P. Rashidi (2019). "Accuracy of Samsung Gear S Smartwatch for Activity Recognition: Validation Study." *JMIR mHealth and uHealth* 7 (2), e11270.

Dinev, T. and P. Hart (2006). "An Extended Privacy Calculus Model for E-Commerce Transactions." *Information systems research* 17 (1), 61–80.

Dinev, T., H. Xu, J. H. Smith, and P. Hart (2013). "Information Privacy and Correlates: An Empirical Attempt to Bridge and Distinguish Privacy-Related Concepts." *European Journal of Information Systems* 22 (3), 295–316.

Filippoupolitis, A., W. Oliff, B. Takand, and G. Loukas (2017). "Location-Enhanced Activity Recognition in Indoor Environments Using Off the Shelf Smart Watch Technology and BLE Beacons." *Sensors*.

Fletcher, R. and S. Park (2017). "The Impact of Trust in the News Media on Online News Consumption and Participation." *Digital journalism* 5 (10), 1281–1299.

Fornell, C. and D. F. Larcker (1981). "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error." *Journal of Marketing Research* 18 (1), 39–50.

George, J. F. (1996). "Computer-Based Monitoring: Common Perceptions and Empirical Results." *Mis Quarterly*, 459–480.

Gorm, N. and I. Shklovski (2016). "Sharing Steps in the Workplace: Changing Privacy Concerns Over Time." In: *Proc. of the 34th Annual CHI Conference on Human Factors in Computing Systems (CHI)*, pp. 4315–4319.

Häikiö, J., J. Kallio, S.-M. Mäkelä, and J. Keränen (2020). "Iot-Based Safety Monitoring From the Perspective of Construction Site Workers." *International Journal of Occupational and Environmental Safety* 4 (1), 1–14.

Hair, J. F., W. C. Black, B. J. Babin, and R. E. Anderson (2014). "Multivariate data analysis: Pearson new international edition." *Essex: Pearson Education Limited* 1, 2.

Hobert, S. and M. Schumann (2018). "Bridging the Gap between Research and Practice: Ten Lessons Learned about Enterprise Wearable Computer Systems." In: *Proc. of the 24th Americas Conference on Information Systems (AMCIS)*.

Hu, L. and P. M. Bentler (1999). "Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives." *Structural equation modeling: a multidisciplinary journal* 6 (1), 1–55.

Huang, C. and Y.-S. Kao (2015). "UTAUT2 Based Predictions of Factors Influencing the Technology Acceptance of Phablets by DNP." *Mathematical Problems in Engineering* 2015.

Huang, C., Y. Wang, T. Wu, and P. Wang (2013). "An Empirical Analysis of the Antecedents and Performance Consequences of Using the Moodle Platform." *International Journal of Information and Education Technology* 3 (2), 217.

Jacobs, J. V., L. J. Hettinger, Y.-H. Huang, S. Jeffries, M. F. Lesch, L. A. Simmons, S. K. Verma, and J. L. Willetts (2019). "Employee Acceptance of Wearable Technology in the Workplace." *Applied ergonomics* 78, 148–156.

Jernejcic, T. and O. El-Gayar (2021). "The Role of Privacy within the Realm of Healthcare Wearables' Acceptance and Use." In: *Proc. of the 27th annual Americas Conference on Information Systems (AMCIS)*.

Kalckreuth, N. von and M. A. Feufel (2021). "Disclosure of Health Data–Conceptualizing the Intention to use Wearables as an Extended Privacy Calculus." In: *Proc. of the 27th annual Americas Conference on Information Systems (AMCIS)*.

Khakurel, J., H. Melkas, and J. Porras (2018). "Tapping Into the Wearable Device Revolution in the Work Environment: A Systematic Review." *Information Technology & People* 31 (3), 791–818.

Khakurel, J., S. Pöysä, and J. Porras (2016). "The Use of Wearable Devices in the Workplace-a Systematic Literature Review." In: *Proc. of the 2nd International Conference on Smart Objects and Technologies for Social Good (GOODTECHS)*, pp. 284–294.

Kim, K. J. and D.-H. Shin (2015). "An Acceptance Model for Smart Watches: Implications for the Adoption of Future Wearable Technology." *Internet Research* 25 (4), 527–541.

Kline, R. B. (2016). *Principles and practice of structural equation modeling*. Fourth edition. Methodology in the social sciences. New York.

Korczynski, M. (2000). "The Political Economy of Trust." *Journal of Management Studies* 37 (1), no–no.

Laufer, R. S. and M. Wolfe (1977). "Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory." *Journal of social Issues* 33 (3), 22–42.

Li, H., J. Wu, Y. Gao, and Y. Shi (2016). "Examining Individuals' Adoption of Healthcare Wearable Devices: An Empirical Study From Privacy Calculus Perspective." *International journal of medical informatics* 88, 8–17.

Li, J., Q. Ma, A. H. Chan, and S. Man (2019). "Health Monitoring Through Wearable Technologies for Older Adults: Smart Wearables Acceptance Model." *Applied ergonomics* 75, 162–169.

Lingg, E., G. Leone, K. Spaulding, and R. B'Far (2014). "Cardea: Cloud Based Employee Health and Wellness Integrated Wellness Application with a Wearable Device and the HCM Data Store." In: *Proc. of the 1st IEEE World Forum on Internet of Things (WF-IoT)*, pp. 265–270.

Maltseva, K. (2020). "Wearables in the Workplace: The Brave New World of Employee Engagement." *Business Horizons*.

McDonald, A. M. and L. F. Cranor (2008). "The Cost of Reading Privacy Policies." *A Journal of Law and Policy for the Information Society (ISJLP)* 4, 543.

McKnight, D. H. and N. L. Chervany (2001). "What Trust Means in E-Commerce Customer Relationships: An Interdisciplinary Conceptual Typology." *International journal of electronic commerce* 6 (2), 35–59.

Mekruksavanich, S., N. Hnoohom, and A. Jitpattanakul (2018). "Smartwatch-Based Sitting Detection With Human Activity Recognition for Office Workers Syndrome." In: *2018 IEEE International ECTI Northern Section Conference on Electrical, Electronics, Computer and Telecommunications Engineering (ECTI-NCON)*, pp. 160–164.

Mettler, T. and J. Wulf (2019). "Physiolytics at the Workplace: Affordances and Constraints of Wearables Use From an Employee's Perspective." *Information Systems Journal* 29 (1), 245–273.

Meyers, N. (2003). "Employee Privacy in the Electronic Workplace: Current Issues for IT Professionals." In: *Proc. of the 14th Australasian Conference on Information Systems (ACIS)*, pp. 72–81.

Naous, D., V. Kulkarni, C. Legner, and B. Garbinato (2019). "Information Disclosure in Location-based Services: An Extended Privacy Calculus Model." In: *Proc. of the 40th International Conference on Information Systems (ICIS)*.

Petronio, S. (2002). *Boundaries of Privacy: Dialectics of Disclosure*.

Prawiro, E. A. P. J., N.-K. Chou, M.-W. Lee, and Y.-H. Lin (2019). "A Wearable System That Detects Posture and Heart Rate: Designing an Integrated Device With Multiparameter Measurements for Better Health Care." *IEEE Consumer Electronics Magazine*.

Princi, E. and N. C. Krämer (2019). "Acceptance of Smart Electronic Monitoring at Work as a Result of a Privacy Calculus Decision." In: *Informatics*. Vol. 6. 3. Multidisciplinary Digital Publishing Institute, p. 40.

Schall Jr, M. C., R. F. Sesek, and L. A. Cavuoto (2018). "Barriers to the Adoption of Wearable Sensors in the Workplace: A Survey of Occupational Safety and Health Professionals." *Human factors* 60 (3), 351–362.

Sen, S., K. K. Rachuri, A. Mukherji, and A. Misra (2016). "Did You Take a Break Today? Detecting Playing Foosball Using Your Smartwatch." In: *Proc. of the 14th IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom)*.

Shoaib, M., S. Bosch, H. Scholten, P. J. M. Havinga, and O. D. Incel (2015). "Towards Detection of Bad Habits by Fusing Smartphone and Smartwatch Sensors." In: *Proc. of the 2015 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom)*.

Smith, H. J., T. Dinev, and H. Xu (2011). "Information Privacy Research: An Interdisciplinary Review." *MIS quarterly*, 989–1015.

Statistisches Bundesamt (Destatis) (2021). *12111-0004: Bevölkerung (Zensus): Deutschland, Stichtag, Geschlecht, Altersgruppen*. URL: `https://www-genesis.destatis.de/genesis/online` (visited on 07/21/2021).

Tirabeni, L. (2020). "Technology, Power, and the Organization: Wearable Technologies and Their Implications for the Performance Appraisal." In: *Performance Appraisal in Modern Employment Relations*, pp. 61–85.

Tomczak, D. L., L. A. Lanzo, and H. Aguinis (2018). "Evidence-Based Recommendations for Employee Performance Monitoring." *Business Horizons* 61 (2), 251–259.

Ur, B., M. Sleeper, and L. F. Cranor (2012). "Privacy, Privacidad, Policies in Social Media: Providing Translated Privacy Notice." In: *Proc. of the 1st Workshop on Privacy and Security in Online Social Media (PSOSM)*.

Wang, T., T. D. Duong, and C. C. Chen (2016). "Intention to Disclose Personal Information via Mobile Applications: A Privacy Calculus Perspective." *International Journal of Information Management* 36 (4), 531–542.

Weinhard, A., M. Hauser, and F. Thiesse (2017). "Explaining Adoption of Pervasive Retail Systems with a Model based on UTAUT2 and the Extended Privacy Calculus." In: *Proc. of the 21st Pacific Asia Conference on Information Systems (PACIS)*, pp. 217–229.

Westin, A. F. (1967). *Privacy and Freedom*. Atheneum.

Weston, M. (2015). "Wearable Surveillance – a Step Too Far?" *Strategic HR Review* 14 (6), 214–219.

Wieneke, A., C. Lehrer, R. Zeder, and R. Jung (2016). "Privacy-Related Decision-Making in the Context of Wearable Use." In: *Proc. of the 20th Pacific Asia Conference on Information Systems (PACIS)*.

Xu, H., H. Teo, B. Tan, and R. Agarwal (2009). "The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services." *Journal of management information systems* 26 (3), 135–174.

Zenker, S. and S. Hobert (2019). "Design and Implementation of a Collaborative Smartwatch Application Supporting Employees in Industrial Workflows." In: *Proc. of the 27th European Conference on Information Systems (ECIS)*.

Ziegler, J., S. Heinze, and L. Urbas (2015). "The Potential of Smartwatches to Support Mobile Industrial Maintenance Tasks." In: *Proc. of the 20th Conference on Emerging Technologies Factory Automation (ETFA)*.