GEORG-AUGUST-UNIVERSITÄT
GÖTTINGEN IN PUBLICA COMMODA SEIT 1737

EMPLOYEES' ACCEPTANCE OF SMART WATCHES IN GERMANY

Privacy-preserving Solutions for Employees and Recommendations for Employers during the Deployment of Smart Watches in Smart Workplaces

DISSERTATION

to obtain the Doctoral Degree (Dr. rer. pol.)
of the Faculty of Economic Sciences
of the Georg-August-Universität Göttingen

submitted by

Alexander Richter
M. Sc. in Technical Business Administration
born in Gifhorn, Germany

Göttingen, 2023

Thesis Committee
First Supervisor: Prof. Dr. Matthias Schumann
Second Supervisor: Prof. Dr.-Ing. Delphine Reinhardt
Third Supervisor: Prof. Dr. Manuel Trenz

Day of the oral examination: 13.09.2023

ABSTRACT

More and more companies rely on smart watches in their processes and equip their employees with them. Smart watches promise a variety of benefits for both employers and employees. These include simplifying information access, promoting employee health, and enhancing occupational safety. While smart watches may offer several benefits, the collection and processing of data collected using their embedded sensors pose several risks to the wearers' privacy, as their employer can obtain information about them and their environment. Moreover, smart watches are continuously worn and thus generate a continuous data flow, which employees may interpret as a privacy invasion by their employers. This can lead to stress and reduced productivity, especially when employees consider privacy risks.

According to regulations, employers must process personal data lawfully and transparently. Therefore, employers have to provide employees with all the necessary information. However, employees may underestimate privacy risks resulting from a lack of awareness or knowledge. Nevertheless, once an agreement has been reached between the employee or works council and the employer, data collection can occur under local laws.

This thesis examines employees' privacy perspectives on potential smart watch data disclosure with the goal to elaborate recommendations for employers alongside the introduction of smart watches in company processes. Furthermore, it explores factors that may influence employees' willingness to share smart watch data and examines their preferences for newly introduced privacy indicators and interactions to stop smart watch data collection. Moreover, we analyze the application of spatial cloaking on employees' location submitted by smart watches and the effect on the productivity of self-driving vehicles. This thesis includes (1) the foundation of our research, (2) our research objectives, (3) the methodology we used to evaluate the outcomes of our research, as well as (4) the evaluation results.

This thesis provides insights for employers about employees' knowledge and preferences regarding smart watch deployments in company processes. Moreover, it derives recommendations for employers at different steps of introducing and using smart watches in smart workplaces. Finally, it proposes different privacy indicators and interactions for employees.

ZUSAMMENFASSUNG

Immer mehr Unternehmen setzen in ihren Prozessen auf Smartwatches und statten ihre Mitarbeiter damit aus. Smartwatches versprechen sowohl für Arbeitgeber als auch für Arbeitnehmer eine Vielzahl von Vorteilen. Dazu gehören die Vereinfachung des Informationszugangs, die Förderung der Mitarbeitergesundheit und die Verbesserung der Arbeitssicherheit. Smartwatches bieten zwar zahlreiche Vorteile, doch die Erfassung und Verarbeitung von Daten, die mit Hilfe ihrer eingebetteten Sensoren gesammelt werden, birgt einige Risiken für die Privatsphäre der Träger, da ihr Arbeitgeber Informationen über sie selbst und ihr Umfeld erhalten kann. Darüber hinaus werden Smartwatches ständig getragen und generieren somit einen kontinuierlichen Datenfluss, was von den Arbeitnehmern als Eingriff in die Privatsphäre durch ihre Arbeitgeber interpretiert werden kann. Dies kann zu Stress und Produktivitätseinbußen führen, insbesondere wenn die Arbeitnehmer die Risiken für die Privatsphäre bedenken.

Gemäß den Vorschriften müssen Arbeitgeber personenbezogene Daten rechtmäßig und transparent verarbeiten. Daher müssen Arbeitgeber ihren Mitarbeitern alle erforderlichen Informationen zur Verfügung stellen. Es kann jedoch vorkommen, dass Arbeitnehmer die Risiken für die Privatsphäre aufgrund mangelnden Bewusstseins oder Wissens unterschätzen. Sobald jedoch eine Vereinbarung zwischen dem Arbeitnehmer oder dem Betriebsrat und dem Arbeitgeber getroffen wurde, kann die Datenerhebung gemäß den lokalen Gesetzen erfolgen.

In dieser Arbeit werden die Datenschutzperspektiven von Arbeitnehmern im Hinblick auf eine mögliche Datenweitergabe durch Smartwatches untersucht, mit dem Ziel, Empfehlungen für Arbeitgeber bei der Einführung von Smartwatches in Unternehmensprozessen zu erarbeiten. Diese Arbeit erforscht Faktoren, welche die Bereitschaft von Arbeitnehmern zur Weitergabe von durch Smartwatches erfassten privaten Daten beeinflussen können, und untersucht ihre Präferenzen für Datenschutzindikatoren und Interaktionen, um die Datenerfassung durch Smartwatches zu stoppen. Darüber hinaus analysieren wir die Anwendung der räumlichen Tarnung auf den von Smartwatches übermittelten Standort des Arbeitgebers und die Auswirkungen auf die Produktivität von selbstfahrenden Fahrzeugen. Diese Arbeit umfasst (1) die Grundlagen unserer Forschung, (2) unsere Forschungsziele, (3) die Methodik, mit der wir die Ergebnisse unserer Forschung evaluiert haben, sowie (4) die Bewertungsergebnisse.

Die vorliegende Arbeit liefert Arbeitgebern Erkenntnisse über das Wissen und die Präferenzen der Mitarbeiter bezüglich des Einsatzes von Smartwatches in Unternehmensprozessen. Darüber hinaus werden Empfehlungen für Arbeitgeber in den verschiedenen Phasen der Einführung und Nutzung von Smartwatches an intelligenten Arbeitsplätzen abgeleitet. Abschließend werden verschiedene Indikatoren für den Schutz der Privatsphäre und Interaktionen für Arbeitnehmer vorgeschlagen.

LIST OF APPENDED PAPERS

I. **A. Richter**. Do Privacy Concerns Prevent Employees' Acceptance of Smart Wearables and Collaborative Robots?. Proceedings of the 10th Fachtagung Sicherheit, Schutz und Zuverlässigkeit (SICHERHEIT), 2020.

II. **A. Richter**, P. Kühtreiber, D. Reinhardt. Exploration of Factors that can Impact the Willingness of Employees to Share Smart Watch Data with their Employers. Privacy and Identity Management. Between Data Protection and Security, 2022.

III. **A. Richter**, P. Kühtreiber, D. 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.

IV. **A. Richter**, P. Kühtreiber, D. Reinhardt. Enhanced Privacy in Smart Workplaces: Employees' Preferences for Transparency Indicators and Control Interactions in the Case of Data Collection with Smart Watches. Proceedings of the 37th International Conference on ICT Systems Security and Privacy Protection (IFIP SEC), 2022.

V. **A. Richter**, A. Reinhardt, and D. Reinhardt. Privacy-Preserving Human-Machine Co-Existence on Smart Factory Shop Floors. Proceedings of the 2nd International Workshop on Simulation Science. (SimScience 2019), 2020.

COMMENTS ON MY PARTICIPATION

PAPER I. I am the sole author of the paper. Delphine Reinhardt has provided valuable advice on my ideas leading to a fruitful discussion and an improvement of the paper.

A. Richter 100%

PAPER II. I am the main author of this paper. Besides writing, my task was to design, create and implement the online study and to evaluate and discuss the obtained results. Delphine Reinhardt has advised me in designing the study, helped in structuring the paper, and writing it. Patrick Kühtreiber has also contributed in improving its writing.

A. Richter 80% | P. Kühtreiber 10% | D. Reinhardt 10%

PAPER III. I am the main author of this paper. My tasks covered conceptualizing and conducting the study, statistical analysis, and writing down the results. Delphine Reinhardt enhanced the paper by advising me on the study design and the structure of the paper and helped in writing the paper. Patrick Kühtreiber helped with writing and adding valuable literature.

A. Richter 80% | P. Kühtreiber 10% | D. Reinhardt 10%

PAPER IV. I am the first author of this paper. I have been responsible for designing the prototypes and for planning and conducting the online study. I performed the statistical analyses and wrote up the collected findings. Patrick Kühtreiber helped in writing and structuring the manuscript and discussing the obtained results. Delphine Reinhardt guided me in designing both the prototypes and study and helped in writing the final manuscript.

A. Richter 80% | P. Kühtreiber 10% | D. Reinhardt 10%

PAPER V. I am the main author of this paper and responsible for the simulation implementation, the results evaluation, and writing the main parts of the paper. Andreas Reinhardt and Delphine Reinhardt have contributed to the writing by introducing sections and improving the paper through recommendations, guidance, and valuable discussions.

A. Richter 75% | A. Reinhardt 15% | D. Reinhardt 10%

ACKNOWLEDGMENTS

First and foremost, I would like to thank my thesis advisory committee, Prof. Dr. Matthias Schumann, Prof. Dr.-Ing. Delphine Reinhardt, and Prof. Dr. Manuel Trenz for all their support, guidance and feedback I received through out the years on my research. A special thanks goes to my second supervisor Prof. Dr.-Ing. Delphine Reinhardt, who allowed me to start the journey to get the PhD through my employment at the Institute of Computer Science and her trust in me. I am grateful for the opportunity I received and that you always encouraged me with the greatest commitment. I would also like to thank her for her helpful insights and her benevolent patience, which have guided me to the point of being able to defend my dissertation. I further thank my supervisor, Prof. Dr. Matthias Schumann, for enabling me to start my PhD at the Georg-August University of Göttingen as an external in his research group and for all the advice I received. Besides, I also appreciate Prof. Dr. Manuel Trenz for his helpful advice.

Beyond that, I would like to thank my former colleagues from the Chair of Computer Security and Privacy and the other Chairs of the Institute of Computer Science at the Georg-August University of Göttingen. They contributed not only to the success of my dissertation through many fruitful discussions and pleasant teamwork but also made my life in Göttingen more enjoyable. These are, in particular, Lindrit Kquiku, Patrick Kühtreiber, Luca Hernandez-Acosta, Dr. Jan Tolsdorf, Dr. Alexander Railean, Chathurangi Wickramasinghe, Dr. Hang Zhang, Dr. Arne Bochem, Dr. Milad Ayoub, Prof. Dr. Benjamin Leiding, Dr. Ella Albrecht, and Prof. Dr. Patrick Harms. Many of them I call my friends today. In this regard, I would like to emphasize my co-authors Prof. Dr. Andreas Reinhardt and Patrick Kühtreiber. Thank you for your valuable input in form of discussions, reviews, and enjoyable co-working, while contributing to my research. Furthermore, I would like to thank Patricia Nitzke, who actively and patiently supported me in many administrative activities.

Apart from my colleagues, I would like to express my thanks to all my friends for being there for me and for their encouragement. At least, a sincere thanks belong to my parents and my family for supporting me during my studies and my PhD. Until the end, you always believed in me and my chosen paths.

September, 2023 Alexander Richter

CONTENTS

LIST OF TABLES

LIST OF ACRONYMS

AGV	Automated Guided Vehicle
AVE	Average Variance Extracted
BDSG	Bundesdatenschutzgesetz
BetrVG	Betriebsverfassungsgesetz
CPM	Communication Privacy Management
CFA	Confirmatory Factor Analysis
EU	European Union
GDPR	General Data Protection Regulation
GPS	Global Positioning System
NFC	Near Field Communication
POS	Point of Sale
SEM	Structural Equation Modeling

TAM	Technology Acceptance Model
TET	Transparency Enhancing Technologies
UTAUT	Unified Theory of Acceptance and Use of Technology

1 INTRODUCTION

1.1 MOTIVATION

An increasing number of smart watches are sold worldwide and this trend is expected to continue in the next years [16, 33]. Apart from being used for private purposes by various users, companies evenly recognize smart watch' potentials and increasingly equip their employees with them [58, 113]. Integrated into processes smart watches can support employees in carrying out their work and increasing their productivity [58, 88, 95]. Moreover, employees can benefit from smart watches due to their unique characteristics [1], including their permanent availability, ease of use, and attachment to the body. This allows almost hands-free and faster access to information and thus supports mobile processes [47, 76, 95, 114, 116]. For example, smart watches can support employees working at assembly lines, alerting them about specific requirements and tasks to execute next [6] or support employees in finding and collecting goods in warehouses [24, 69]. Besides, smart watch embedded sensors can promote employees' health and well-being [34, 36, 52] or increase occupational safety [10, 21].

While smart watches may offer several benefits, the collection and processing of data collected using their embedded sensors pose several risks to the wearers' privacy, as information about themselves and their environment can be obtained [3, 70]. Smart watches can determine and track wearers' location [30] or recognize current activity based on sensor data [26, 65]. Therefore, employers can use smart watch data to check whether the employees are at their workplace [89], to track their smoking behavior [91], or to infer the employees' general health [78] and emotions [97]. Furthermore, smart watches are usually continuously worn, while smartphones and other information systems are not [20]. 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 [67, 102], especially when employees consider privacy risks. Hence, smart watches can be seen as a surveillance tool deployed by employers and therefore employers face new challenges concerning employees' privacy [48].

As these devices collect various data about their wearers, they pose potential risks to the wearer's privacy. Such risks may reduce the employees' acceptance. This may be exacerbated by the power imbalance between employees and employers, as employees generally cannot opt-out but would likely do so if they could [48]. Therefore, it is recommended that companies record only work-related data and establish transparent processes to optimize the balance between advantages and associated risks [102]. However, based on law, employers are only allowed to gather personal data, if they are necessary for the existing employment relationship (Bundesdatenschutzgesetz (BDSG), Sec. 32). Before they can legally collect and analyze employees' data employers need to seek employees' consent in advance [12]. This usually requires employees' acceptance to use such devices [42], which potentially benefits both employers and employees. As a result, this highlights the importance of the employees' opinions and decisions. However, collective agreements between employers and employees are legally possible to bypass

individual employees' decision. Such collective agreements are generally negotiated between employers and works councils. However, not every companies' workforce has a works council, which could negotiate on their behalf. For example, it is the case when not at least five permanent employees are employed (Betriebsverfassungsgesetz (BetrVG), Sec. 1). In addition, despite the legal obligation, some companies do not have a works council, as establishing one is often associated with a cost and organizational effort that is difficult to bear. Works councils have the task of implementing applicable laws, ordinances, accident prevention regulations, collective agreements, and company agreements in the interests of the employees (BetrVG, Sec. 80). Especially when the workforce is organized through a works council, the introduction of smart watches, which are designed to collect data from employees, is subject to an additional process. This means that instead of just convincing the employees of the benefits of smart watches, it is first necessary to convince the works council in a preceding step. As soon as the works council has been convinced, employees can be convinced of this in turn or informed about the risks to be expected.

Once employees themselves or the works council have consented to the collection of smart watch data through a collective agreement, employers can collect them according to the signed agreement. In this case, a one-time consent can cause a continuous data collection. Nevertheless, in accordance with the General Data Protection Regulation (GDPR), employers must process personal data lawfully and transparently (GDPR, Art. 5 (1) a)), even though the GDPR leaves the regulations regarding the handling of employee data to the member states (GDPR, Art. 88). In general, the principle of Fair and Transparent Processing requires that the data subject is informed about the collection of personal data (GDPR, Recital 60). Hence, the importance of treating employees fairly is beyond question, when employers consider smart watch deployment. Therefore, employers should provide employees with all necessary information, in order to enable employees to make an informed decision. Otherwise, works councils can negotiate a collective agreement with all necessary information. Such information can include details about data collection, usage, and storage. However, privacy policies have been shown to be challenging to understand [80, 105] and often ignored [62]. Additionally, employees may underestimate the privacy risks resulting from the smart watches, due to a lack of awareness and knowledge [80]. The lack of knowledge often increases users' privacy concerns, thus negatively influencing users' intention to disclose sensitive data. Such effects of privacy concerns on users' intentions were shown in different areas [29, 45, 103, 115]. Whereas with knowledge about the collection and use of private data people tend to be less concerned about their privacy [41, 79].

Therefore, this thesis aims to highlight employees' privacy perspectives on potential smart watch data disclosure with the goal to elaborate recommendations for employers alongside the introduction of smart watches in company processes. To this end, we analyze existing research and derive a set of research questions. Based on them, we explore factors that may influence employees' willingness to share smart watch captured private data. We investigate the effects of employers' provided information on employees' intention to share information when equipped with a smart watch. We examine employees' preferences for different proposed privacy indicators to raise their awareness about current data collection as well as various smart watch interactions to stop ongoing data collection. Moreover, we analyze the appliance of spatial cloaking on employers' location submitted by smart watches and the effect on the productivity of self-driving vehicles. Based on our insights, we recommend that employers, should

1. Consider employees' knowledge about smart watches and legislation knowledge before the planned smart watch introduction. Moreover, they should develop methods to bridge potential knowledge gaps.

2. Provide employees with comprehensible information during the smart watch introduction. Likewise, they should provide privacy solutions to mitigate negative influences due to privacy risks.

3. Implement valuable privacy indicators and interactions on smart watches to allow employees to stop data collection temporarily when smart watch data is already used. Besides, employers should find the best parameters for their workplace setting when using smart watch data to locate workers for Automated Guided Vehicle (AGV) routing to achieve both workplace safety and AGVs' productivity. Moreover, AGVs could use previous workers' locations until a new one has been transmitted.

The remainder of this thesis is structured as follows: Chapter 1 continues with Section 1.2, which provides an overview of the research background by introducing basic terms and elaborating on legal aspects. Section 1.3 specifies the thesis research objectives and presents the three research questions that serve as the basis for this thesis. Section 1.4 presents the structure of the thesis and explains the arrangement and relation of the appended papers. Section 1.5 provides an overview and explanation of the applied methodology. Section 1.6 gives a summary of appended Papers I-V, followed by the respective paper in Chapters 2 to 6. Chapter 7 highlights our contributions by summarizing our results, showing their implications, and discussing their limitations. Chapter 8 concludes the thesis and provides an outlook for future research.

1.2 BACKGROUND

This section provides a foundation for the research background considered in this thesis by introducing the basics of privacy (Section 1.2.1), privacy research at workplaces (Section 1.2.2), legal frameworks (Section 1.2.3), transparency (Section 1.2.4), control (Section 1.2.5), Automated Guided Vehicle (Section 1.2.6) and smart watch (Section 1.2.7). Moreover, it addresses privacy risks due to sensors in Section 1.2.8.

1.2.1 *Privacy*

In this thesis, we rely on the concept of privacy, which refers to "informational privacy" and is applied in workplace scenarios considering employment situations between employees and employers in German companies. This concept of privacy was formerly established by Westin in 1967 [108]. Westin describes privacy as: "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" [108]. Thereby, informational privacy considers the influence of ongoing technological development and is related to the individual power to control disclosing or withholding their information from others. Apart from this definition, workplace privacy or organizational privacy, "is defined as a state or condition in which the individual has the capacity to (a) control the release and possible subsequent dissemination of information about him or herself, (b) regulate

both the amount and nature of social interaction, (c) exclude or isolate him or herself from unwanted (auditory, visual, etc.) stimuli in an environment, and, as a consequence, can (d) behave autonomously (i.e., free from the control of others)" [96]. However, this definition encompasses various privacy dimensions like "autonomy privacy", "work environment privacy", and "information privacy", which are to some extent intermingled [12, 96]. Bhave, Teo, and Dalal [12] described this intermingling as if employees could not exert control over their physical workspace (work environment privacy), they might not be able to control whether and when they want to interact with their colleagues (autonomy privacy), thus potentially resulting in their inability to control the information collected about them (information privacy). However, only the last dimension, information privacy, refers to Westin's formerly introduced definition of privacy.

In recent years research also adapted this concept of privacy to the employment context. Privacy in employment "entails (perceptions of) control over the acquisition, storage, use, dissemination, and dispersal of employees' data. That is, it concerns control over the information that could be made available to others" [12].

1.2.2 *Privacy research in workplaces*

Research on privacy in workplaces is diverse. The research deals with, e.g., privacy perceptions, workplace monitoring and surveillance, and privacy solutions like dashboards.

Various studies have obtained extensive insights into employees' privacy perceptions, particularly regarding the influence of their privacy concerns on their intention to use an information system [18, 19, 27, 49, 55, 66, 80]. In this regard, researchers often rely on theoretical models, such as Technology Acceptance Model (TAM), Unified Theory of Acceptance and Use of Technology (UTAUT), Communication Privacy Management (CPM), and privacy calculus, or explore employees' mental models. While TAM and its additions, such as UTAUT, tend to explain the acceptance of information technologies in the workplace context, CPM and privacy calculus focus on explaining employee behavior based on an internal mental calculus that results from the disclosure or concealment of private information [2, 29]. In comparison, mental model research serves to understand employees' perceptions, thoughts, beliefs, and decisions. In this context, a mental model is an idea or image about certain concepts, objects, or situations and can significantly influence perceptions, thoughts, beliefs, and decisions [85]. Through the use of these theoretical models, researchers found across a wide variety of domains in the workplace context that employees' privacy concerns may negatively impact perceived usefulness, ease of use, and attitudes toward technology, which in turn reduces employees' intention to use it [18, 27, 49, 55]. The authors in [100] examined the correlations between employees' perceptions of data privacy, their sensitivity in dealing with personal data, and their willingness to disclose this data. Their findings indicate that positive attitudes toward technology and high trust in employers are associated with a higher willingness to disclose personal data, while privacy concerns lead to a lower willingness to do so. Other researchers, using the privacy calculus, found that privacy concerns reduce employees' intention to use employee analytics [19] whereas benefits such as improving performance or job security while protecting privacy lead to acceptance of smart electronic monitoring systems [80]. In examining mental models, the authors in [99] revealed that most employees have a basic understanding of the concept of the right to informational self-determination. However, the understanding of it is influenced by

various factors like trust in the employer, the type of information processed, and control over the use of that information. In another study, the authors in [66] examine employees' mental models of wearables in the workplace. They found that these are shaped by fear of privacy intrusions and fear of limited self-determination. Consequently, high levels of privacy concerns hindered the adoption of wearables. However, some employees were generally willing to disclose data if they received adequate consideration.

Another area of workplace privacy is workplace monitoring and surveillance. Employers have various reasons for implementing technology-enabled surveillance and monitoring, such as improving productivity [7]. However, monitoring can be considered an invasion of privacy [63]. Research has focused primarily on the impact of monitoring on a wide variety of factors, such as job satisfaction or perceived stress [7, 92, 107]. The study in [107] showed that monitoring and surveillance to deter undesirable behavior was associated with lower employee satisfaction. Similar findings can be found in [7] and [92]. The authors in [7] identified 85 studies and processed them qualitatively and meta-analytically. In addition to lower employee satisfaction, they also found negative effects of monitoring on perceived stress, psychological strain, trust in the organization, and perceived control. The authors in [92] also found a negative effect on job satisfaction and stress in their study with data from 70 independent samples. However, apart from these findings on the influence of employee monitoring, research exists that provides recommendations for employee monitoring [101]. The authors use theory and empirical research findings to derive five recommendations for maximizing the positive effects of monitoring while minimizing the negative ones.

In addition to the studies on workplace monitoring, various researchers deal with implementing the rights of the employees concerned by examining, for example, the use of so-called privacy dashboards [77, 86]. The authors in [77] examine employees' demands for transparency and self-determination when implementing corporate privacy dashboards. They found that employees want, among other things, insights into the stored data and the underlying authorization system. They derived requirements and data usage models to implement data protection dashboards. Whereas, the authors in [86] developed "MyData" dashboard for employees to have more visibility and control over personal data processed through business processes, for example. They found that employees experienced better control over their personal data through the dashboard.

1.2.3 *Legal Frameworks*

To empower individuals in their rights, various privacy laws were developed and established worldwide. For European citizens, the GDPR was established in May 2018 and is the mandatory privacy law in all European Union (EU) member states and applies insofar as, e.g., data of EU citizens are stored or processed. With regard to privacy in employment the GDPR is also binding. However, as the GDPR allows Member States to "provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context" (GDPR, Art. 88 (1)), further laws can specify the GDPR within the individual European countries. This results in regional differences in the definition and interpretation of the right to privacy in the employment context. Hence, regulations in an employment context are a combination of national and European laws and regulations. For example, in Germany, the GDPR, BDSG and the Betriebsverfassungsgesetz (BetrVG) are binding for employers in this context.

In addition to the statutory regulations, various supervisory authorities and bodies are important to monitor the application of employee data protection regulations. These include independent public supervisory authorities (GDPR, Art. 51) or organizational dependent Data Protection Officers and works councils. While supervisory authorities like Germany's Freedom of Information or State Commissioners for Data Protection were established to allow employees to report data privacy violations to an independent public authority, the latter are internal organizational bodies to avoid and resolve privacy issues. Data Protection Officers are designated by employers and can be considered as their representatives (GDPR, Art. 37) and should be involved in cases related to personal data protection. Although employers must appoint the Data Protection Officers under certain conditions (GDPR, Art. 37 and BDSG Sec. 38), the Data Protection Officers are not subject to the employer's instructions in performing their duties and may not be punished or dismissed for their duties (GDPR, Art. 38 (2)). In comparison, the works councils have, in accordance with Sec. 80 (1) No. 1 BetrVG the duty "to see that effect is given to acts, statutory instruments, safety regulations, collective agreements, and works agreements for the benefit of the employees". In addition, employers have to incorporate works councils, say whenever employers plan "the introduction and use of technical devices designed to monitor the behavior or performance of the employees" (BetrVG, Sec. 87 (1) No. 6).

The legislator also considers various actors and stakeholders, which are involved in personal data flow and processing (GDPR, Art. 4). These are the data subjects, recipients, controllers, processors, or third parties. While a data subject can be any identified or identifiable natural person about which personal data are processed (GDPR, Art. 4 (1)), processors, controllers, and third parties are natural or legal persons, public authorities, agencies, or other bodies. Processors process the personal data on behalf of the controller (GDPR, Art. 4 (6)), which determines the purposes and means of the processing of personal data. In comparison, third parties are authorized to process personal data, although they are not under the direct authority of the controller or processor (GDPR, Art. 4 (10)). In the context of employment, employees are considered as data subjects, and employers as controllers. Processors, in that sense, are employees who have to process collected personal data to fulfill the employers (collectors) obligations by, e.g., determination of taxes in the payroll. Third parties could be customers or suppliers.

Basically, the previously mentioned term "personal data" refers to any information about a person that is able to identify a natural person (GDPR, Art. 4). "In particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" (GDPR, Art. 4). However, processing of personal data is only lawful when, e.g., an employee (data subject) has given his/her consent (GDPR, Art. 6 (1) a and BDSG, Sec. 26 (2)). Whereby a "consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her" (GDPR, Art. 4). In the employment relationship in particular, however, the employees' consent can be questioned, because of their dependency on employers [5]. According to Sec. 26 BDSG, such consent is recognized if the consent is associated with an employee benefit (legal or economic) or if both employees and employers pursue the same interests.

1.2.4 *Transparency*

Transparency is one of the fundamental principles in the GDPR with respect to the processing of personal data (GDPR, Art. 5 (1) a). In general, the principle of Fair and Transparent Processing requires that the data subject is informed about the collection of personal data (GDPR, Recital 60). In detail, the principle requires that information about the processing should not only be easily accessible but also understandable (GDPR, Recital 39, 58). This can be supported by comprehensible visual elements, such as standardized symbols, which can provide an understandable overview of the processing (GDPR, Recital 60). Moreover, data subjects "should be made aware of risks, rules, safeguards and rights in relation to the processing" (GDPR, Recital 39). Transparency is distinguished into ex ante and ex post transparency. While ex ante transparency considers future intended data processing, ex post transparency informs about already performed data processing. Thus, ex ante transparency provides data subjects with all necessary information to make informed decisions about future product or service usage (GDPR, Art. 14), whereas ex post transparency enables a user to subsequently obtain information about processed data (GDPR, Art. 13). To enable users to exercise their rights to transparency and technology-enabled intervention capabilities, various Transparency Enhancing Technologies (TET) have been developed.

Ex ante TETs present privacy information in, e.g., privacy policies. Such information should be machine-readable to support electronic statements [73]. The browser add-on Privacy Bird searches for such privacy policies, compares them with predefined users' privacy preferences, and indicates in an easily understandable traffic light system whether they are met or not [43]. Besides, privacy policies may be combined with standardized icons to provide users with simple understandable visuals to help them understand the most relevant implications of the most difficultly readable privacy policies more easily [43, 73]. Mozilla Privacy Icons, for example, reduce the complexity of privacy policies by translating and visualizing them with the help of icons [43].

Ex post TETs present insight into performed data processing and raise awareness about it. Ex post TETs use, among others, textual information, color, graphical elements, or maps to visualize disclosed sensitive data [8, 14, 72]. Privacy Leaks, e.g., provide insights about smartphone application data usage using color codes and text elements [8]. Whereas other solutions like geographical boundaries [72] or geographical heat maps [14] use maps to visualize frequently visited areas to raise awareness of the locations processed. Further TET examples can be found in [43, 73].

Regarding transparency in an employment relationship, employees have the same rights as data subjects in case of intended processing or processed data. Thus, employers have to provide comprehensive information on the processing of employees' personal data.

1.2.5 *Control*

Transparency is often associated with control over personal data or the intervenability of processing personal data by the data subjects themselves. Based on the GDPR, data subjects have the right to rectification (GDPR, Art. 16), erasure (GDPR, Art. 17), and restriction of processing (GDPR, Art. 19) of their data. In addition, a data subject has the right to object (GDPR, Art. 21). This allows the data subject to revoke their consent to the processing

at any time. These rights allow control over the data as soon as it has been collected. However, such rights can only be exercised if the data subject has proven knowledge about processed data [64, 73]. The same applies in the broadest sense to employees for the personal data processed by employers. For German employees, the rights of the data subjects (BDSG, Sec. 32 - 37) and the employee rights under labor law (BetrVG, Sec. 83) apply. Apart from the rights to information and access to personal data or rights to data correction, employees have the right not to be subject to a decision based solely on automated processing (including profiling) (GDPR, Art. 22). This right in accordance with Art. 22 GDPR only applies if the automated processing is either not necessary, is not legally permissible, or there is no employees' consent. Even if employees' consent is given, employees have the ability to enforce their stated rights as mentioned above.

1.2.6 *Automated Guided Vehicle*

Smart factories are characterized by the presence of AGVs and other robots that contribute to industrial processes [37]. AGVs are expected to transport materials between machines and workplaces and their autonomy allows them to collect and deliver items when and where they are needed. For the AGVs' coordination, a large volume of information is collected and exchanged between participating devices. This enables seamless, safe, and secure interactions between humans, machines, material, and systems [54, 81, 112]. Since AGVs move independently between different places, it is of particular importance that AGVs know the positions of the human workers sharing the shop floor in order to reduce their speed or even completely stop in the case of an impending collision. Diverse options exist to proactively prevent collisions between AGVs and workers. Most often, this collision prevention is realized through equipping the autonomous robots with detectors for human presence and stopping their operation while a human is present in their immediate environment. Diverse technologies can support human detection. On the one hand, AGVs can be equipped with infrared sensors to detect body heat, radar sensors or laser rangefinders to recognize the shape of human bodies, or cameras to locate humans and anticipate their movements [40]. Particularly, laser rangefinders are often used to detect obstacles on shop floors [35]. However, in that case, the AGVs could not optimize their trajectories in advance. On the other hand, workers can be equipped with wearable devices that periodically broadcast their current position on the shop floor and thus allow nearby AGVs to stop if they come too close. A strong advantage of the latter type of solutions is their capability to detect workers even when they are not within the camera's field of view.

1.2.7 *Smart watch*

A wearable computer is a small computing device designed to be worn on the body [11, 61]. Wearable computers or smart wearables encompass, e.g. smart glasses, fitness trackers, or smart watches. The latter is the most commonly used wearable computer apart from fitness trackers. As the name smart watch suggests, the device is shaped like an ordinary watch but provides more capabilities and contains computer hardware. Smart watches run with an operating system and are able to execute separately installed applications [83]. However, some smart watches are delimited on the interplay with a connected smart phone [83]. Smart watches are wrist-worn devices, always available, and

able to raise wearers' attention due to various auditory or haptic feedback regardless of time or location [15, 44]. In addition, smart watches are equipped with various sensors, Near Field Communication (NFC), Global Positioning System (GPS), and Bluetooth, and can be operated via touchscreen, buttons, motion gestures, or even voice [13, 23]. However, due to the size factor, smart watches are limited to simple inputs and outputs [59]. Nevertheless, they are able to constantly gather data about the environment or the wearer themselves with sensors like an accelerometer, gyroscope, barometer, and ambient light sensor.

1.2.8 *Risks of Privacy due to Sensors*

As previously mentioned, smart watches are equipped with a wide variety of sensors. Such sensors can be used to measure values related to the wearer and thus represent potential privacy risks, as different inferences can be made about the wearers. As an example, the gait, a person's own walking style, as a behavioral biometric can be used to recognize a specific user [28, 32]. In the following, we consider commonly used sensors, such as (a) accelerometer, (b) gyroscope, (c) barometer, (d) thermistor, and (e) heart-rate sensors and give a brief explanation for each, before referring to the potential associated privacy risks.

(a) Accelerometers are used to measure the acceleration of a device in three different dimensions and allow measures of speed increases and decreases by determining the positional changes. Thus, an accelerometer enables, e.g., the measurement of how an individual moves around in space. Since accelerometers are not precise enough, they are mostly combined with a gyroscope. Accelerometer data can be used for the localization of a user, activity recognition methods, and spy on textual inputs at keyboards, displays, or even on whiteboards as detailed below.

Some authors have illustrated that the accelerometer data can be used to identify a user's location [38, 50]. In [50], the authors show that they are able to determine transitions from selected positions in an office environment using accelerometer data. The authors in [38] show that it is possible to locate the device with the help of the acceleration sensor. With their proof of concept, the authors are able to estimate the actual movement trajectory of a smartphone in a moving vehicle within a radius of 200 m using their collected accelerometer data.

It is also feasible to recognize keystrokes [53, 56, 87, 106]. The project [56] demonstrates the feasibility to recognizing keystrokes on a smartphone with smart watch accelerometers. Combined with a gyroscope, it is also possible to recognize PIN entries on a smartphone while using a smart watch [87]. Furthermore, [106] demonstrates that textual inputs on a keyboard located on a desk can be identified using a smart watch. Based on [53], the built-in sensors in a smart watch allow to recognize text input on a QWERTY keyboard as well as PIN inputs on a Point of Sale (POS) terminal. The authors used the accelerometer in combination with the microphone for this purpose. With the help of a smart watch with an accelerometer, it is also feasible to recognize text handwritten on a whiteboard [4]. In this approach, they recognize 94% of single letters at the first estimate. They also show that the built-in microphone helps to segment letters and thus contributes to their recognition.

Accelerometer data can also be used for activity recognition as shown in, e.g., [9, 82, 93]. The authors in [9] show that it is feasible to recognize a variety of everyday activities with an accuracy rate of 84% when multiple accelerometers are worn simultaneously on different body parts. By using just one accelerometer worn near the pelvic area, the authors in [82] are able to distinguish a variety of activities (e.g., standing, walking, running) with a fairly high degree of accuracy. However, the detection of movements involving only hands or mouth movements are comparatively more difficult to detect. A comparable method is introduced in [93]. They found out that one accelerometer inside the pocket of the subject's trousers allows real-time recognition of his/her activity (e.g., walking, running, cycling, driving) with excellent accuracy.

(b) The gyroscope allows determining the devices' position around three axes. In contrast to the accelerometer, the gyroscope detects the intensity through the rotational movements. The measurements from the gyroscope can be useful for activity recognition and identifying keystrokes on diverse keyboards. A gyroscope in a wearable device can also be used to recognize the human activity. The authors in [91] demonstrate the possibility of identifying seven commonly operated physical activities (e.g., sitting, standing, and biking) with only a smartphone in the pocket, a smart watch on the wrist, or a combination of both. Furthermore, they show that further complex activities like smoking, eating, drinking coffee, giving a talk, typing, and writing can also be recognized with high accuracy by combining the sensors [91].

In addition to the feasibility of recognizing human activities with a gyroscope, it is also possible to use a combination of stereo-microphones and gyroscopes to infer keystrokes on a smartphone with high accuracy, as shown in [74].

(c) A barometer sensor is used to measure the ambient air pressure. With this sensor, even small changes in the ambient air pressure are an indicator of climbing stairs [111]. The measured pressure changes from a barometer can be used to recognize human activities [60].

(d) Thermistors, thermoelectric effects, or optical methods can be used to measure skin temperature [46]. Commonly, the change in resistance is used to measure the temperature [46]. This allows the sensor to detect skin temperature, which is usually a few degrees Celsius below body temperature and highly dependent on ambient temperature [46]. Changes in body temperature may indicate disease. For example, a temperature rise can indicate an infection, or a drop in temperature can indicate a low blood pressure [46]. According to [71], the measurement of temperature variations of the body can be used to detect medical stress that might indicate a stroke or a heart attack. Furthermore, [71] suggests that the body temperature measurement is useful to determine a physiological condition or an activity classification [75, 110].

(e) In order to measure heart rates, two different methods can be used. One is the optical method using light, and the other is the electronic method using electrodes. The optical method, or optical heart rate monitoring, uses a technique known as photoplethysmography, in which the light penetrates the skin and blood vessels. The light is reflected or absorbed by the volume of the blood vessels. Finally, an

optical sensor can measure the reflecting light and determine the current pulse [51, 57]. With the electronic method, electrical heart monitoring or electrocardiogram, the voltage change caused by the heart muscles can be measured with electrodes on the body surface, and thus the pulse can be determined [51, 57]. To notice various internal states of the body as well as arousal states, according to [39], the heart rate variability is a commonly used biosignal. The irregular beats of the heart of a relaxed, healthy person, influenced by breathing and the autonomous nervous system, lead to a constant change in the beats between two intervals. Instead of this, the heartbeat between two intervals of stressed persons becomes more steady and loses variability. From this, it can be concluded that a person is in a state of stress [39]. This was also shown in an approach, where unobtrusive portable sensors were used to detect mental stress by analyzing heart rate variability [22].

Moreover, we consider privacy risks caused by the commonly used technologies (f) Bluetooth and (g) Wi-Fi, although these are not traditional sensors.

(f) Bluetooth is a short-range communication technology and a wireless transmission standard for exchanging data between devices using UHF radio waves. Bluetooth can be used for location tracking. [84] demonstrates a system to communicate with mobile devices using Bluetooth to localize mobile devices in indoor environments. Their approach used the received signal strength at mobile devices from network access points. Servers use previously computed signal strength maps to determine the position of the mobile devices. In order to use the advantages of localization in smart workplaces, some authors present solutions to localize mobile devices using Bluetooth for occupancy or reminders. For example the feasibility to detect office occupancy using Bluetooth signals is shown in [90].

(g) Wi-Fi is a wireless networking standard that uses radio waves to transmit data between devices and operates on a 2.4 and 5 GHz frequency. Several authors demonstrate the possibility of determining the location of devices using it (e.g., [25, 68]). Wi-Fi allow indoor location tracking. [68] demonstrated a location tracking system based on a typically existing Wi-Fi network infrastructure within an organization. Even if their approach is not as accurate as a GPS-based approach, they are able to roughly determine the location of a mobile device.

1.3 RESEARCH OBJECTIVES

In this thesis, we aim at developing privacy-preserving solutions for employees and to elicit recommendations for employers when deploying smart watches in smart workplaces. Hereby, this thesis contributes to the state of knowledge by addressing the following research questions:

RQ 1: Which employees' level of knowledge regarding privacy risks results in acceptance problems?

RQ 2: Which information or conditions influence employees' acceptance?

RQ 3: How do solutions need to be implemented in companies to ensure and enhance employees' privacy?

Research question 1 aims to identify factors that influence employees' willingness to share data about themselves with employers that would be collected using a smart watch. The aim is to identify influencing factors to derive recommendations for employers so that employees can benefit from this through further education. These factors include employees' technical and legal knowledge. Whereby the legal knowledge refers to the applicable laws in Germany concerning data collection in the professional context, such as the GDPR or the BetrVG. In contrast, the technical questions refer to the smart watch' data collection capabilities. Based on this, we will derive directions, where employers could intervene by enlightening about laws or smart watches.

Research question 2 aims to determine the influence of the information provided to employees on their decision to share data with their employer. The aim is to determine whether providing further details on potential risks in the sense of increased transparency leads to an increased willingness of employees to share personal information with the employer. The findings should lead to recommendations for employers to provide employees with more valuable information and not just more information.

Research question 3 aims to investigate solutions that can improve employees' privacy in different ways. Here, the assumption is that employees are equipped with a smart watch that shares personal data about their health conditions, activities made, or the precise location with their employers. It aims to identify, on the one hand, whether solutions can be deployed to improve privacy using obfuscation and, on the other hand, in what form employees desire the proposed solutions in terms of transparency. The results will then be used to derive recommendations for employers.

1.4 STRUCTURE

This section presents the structure of the thesis and explains the arrangement and relation of the appended papers. Thereby, the structure builds on the different steps of smart watch deployments in smart workplaces to develop recommendations for employers to improve employees' privacy by understanding their acceptance of smart watches and implementing mechanisms to enhance employees' privacy. To this end, the thesis focuses on the following three steps for corporate smart watch use:

1. **Before the planned smart watch introduction** based on the exploration of influencing factors
2. **During the introduction of smart watches** based on employers' provided information
3. **During the smart watch use** and the resulting data collection

As a basis for these steps, Paper I motivated the idea, outlined the scope of the thesis, and the research questions (see Section 1.3). The paper considered both smart wearables and collaborative robots as technologies that are components of recent and future digitization of the workplace with the ability to enhance productivity and employees' efficiency. Moreover, both share similarities regarding the embedded sensors, which enable employers to collect, analyze, and draw inferences about the employees. Furthermore, combining several sensor data from different sources might empower employers to gather more insights about employees' sensitive data, e.g., employees' health or job performance. Therefore, both were considered in the early stage of this thesis. However, in the subsequent stages we are focusing only on smart watches. The following explains the arrangement of the other appended papers concerning the previously introduced steps and the research questions. Figure 1.1 shows an overview of the final arrangement.

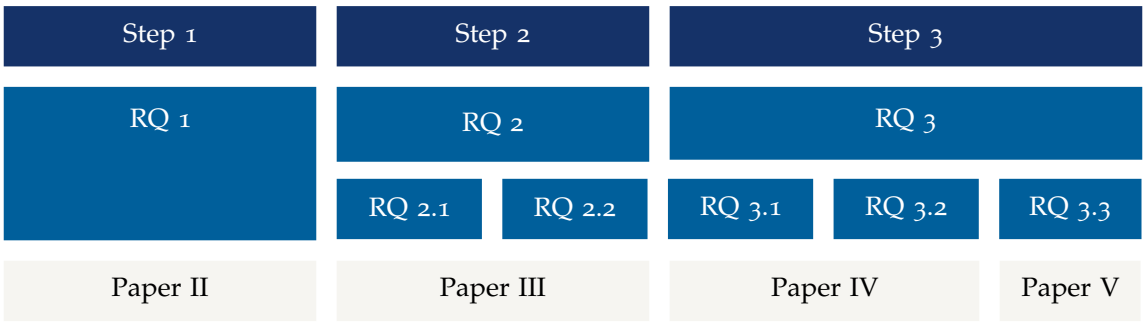


Figure 1.1: Structure of the thesis with explored steps, the connected research questions, and assigned papers

The **first step** represents the moment before smart watches are introduced and encompasses factors that might influence employees' acceptance. This step corresponds to our first research question (*RQ1: Which employees' level of knowledge regarding privacy risks results in acceptance problems?*), aiming to gather first insights about employees' level of knowledge. Paper II considered factors that may influence employees' willingness to share smart watch data to answer this research question. In detail, the paper analyzes the impacts of employees' legislation knowledge, technical knowledge about smart watch capabilities, and technical affinity on employees' willingness to share such information.

The **second step** addresses the influence of information employers provide about smart watches during their introduction. Our second research question about which information or conditions influence employees' acceptance is assigned to this stage. Hence, Paper III examines the effects of employers' provided information on the employees' intention to share information like activity, health, and location when equipped with a smart watch to answer this research question. To address this research question, Paper III answers the following two sub research questions:

RQ 2.1: Does more extensive information provided to the employees increase their willingness to disclose private information to their employer?

RQ 2.2: How does the provision of more extensive information influence the relationship between perceived risk, benefits, and the intention to disclose information?

The **third step** considers smart watches when already in use and data is collected about the employees. To this step, our last research question, about how solutions need to be implemented in companies to protect employees' privacy, is assigned. Both Paper IV and Paper V address this research question. While Paper IV examines employees' preferences for different proposed privacy indicators and interactions to stop this collection, Paper V considers the co-existence of human workers and AGVs on smart factory shop floors and applies a privacy-preserving solution (spatial cloaking). However, both explore privacy-enhancing solutions in different ways. In this regard, Paper IV answers the following sub research questions:

RQ 3.1: Which transparency indicator visualization(s) do employees perceive as sufficient and useful to be informed about the current data collection?

RQ 3.2: Which interaction(s) is/are perceived by the employees as appropriate to control the data collection?

Looking back to the first paper, which deals with smart watches but also collaborative robots, the picture comes full circle, as both robots and smart watches are considered in the last stage. Whereas, Paper IV considers privacy solutions directly on smart watches, Paper V examines the impact of a privacy-enhancing solution used to cloak employees' precise locations for AGVs on workplace safety and AGVs' productivity. In this regard, Paper V answers the following research question.

RQ 3.3: What trade-off exists between employee workplace safety and AGVs' productivity?

1.5 METHODOLOGY

This section details the research methodologies applied throughout this thesis.

1.5.1 *Literature Research*

In all included papers, a literature review has been conducted. The literature reviews cover the current state of the underlying research topics. Various databases were used for the literature research and searched by means of queries. The databases were, among others: ACM Digital Library, AIS Electronic Library, Göttingen University Catalogue (GUK), IEEE Xplore Digital Library, and SpringerLink. Since we focus on Germany, we included both English and German literature. We have especially considered peer-reviewed journals and proceedings as well as books. For the queries, we used the keywords, i.e., privacy, risks, concerns, employees, smart watches, or workplace in various combinations. After removing duplicates, remaining articles were checked for relevance based on their title and abstract first.

1.5.2 *Online Survey*

The findings obtained in Papers II-IV were based on online questionnaires. Their goal in Papers II and III was to explore factors that influence smart watch usage, while the one conducted in Paper IV was to elicit users' preferences for privacy indicators and control mechanisms for smart watches. All online questionnaires in Papers II-IV were reviewed and approved by our data protection officer. The online questionnaires in Papers II and III underwent additional approval by our university's ethics committee. The panel provider we chose for Papers II-IV was ISO 26362 certified and covered participants from seven European countries containing a balanced mix of special target groups and a cross-section of the respective population. This also includes the cross-section of the German population, which is especially interesting, as we focus on fully-employed German employees. All participants were full-time employees working in different sectors in Germany aged 18 years and above. Moreover, both distributions in terms of age and gender are representative of the German population [94]. Besides, all designed online surveys were in German and accessible on mobile devices. Furthermore, for all conducted online surveys, we have taken care to minimize potential harm to the participants by, e.g., reducing the number of questions to the minimum to avoid fatigue. Moreover, participants have been informed that they can leave the questionnaire anytime. Note that all participants were monetarily rewarded for their contributions.

1.5.3 *Simulation*

The goal of Paper V was to elicit parameters for the safe and efficient operation of workers and AGVs by means of a simulation. Thereby, the simulation conducted in Paper V served the purpose to elicit how the specific factors affect the accuracy of detection workers on a shop floor, and also assess the extent to which workers' privacy is preserved. These factors encompass the spatial cloaking radius, spatial cloaking reporting frequency, and transmission success rate. To evaluate the different parameters, we have created a virtual

simulation environment in NetLogo, an agent-based-social framework [98, 109]. In the simulation environment, designed in NetLogo, both workers and AGVs move between different areas. While workers visit both their workplaces and the staff room, AGVs roam between workplace storage units and the main storage room. This setting is applied to simulate a manufacturing setting, in which AGVs regularly deliver new materials to the workplaces and move completed items to the main storage. Our simulation corresponds to a 10 h working day and thus approximately 2 h over the average working hours inside industrial environments. It hence provides a better comparison with real production environments [17, 104]. All simulation results show the average values of three runs with different random seeds.

1.5.4 *Statistical Analysis*

We have used statistical methods in Paper II-V. Quantitative methods were used, as we created comparatively large data sets using online surveys with a standardized questionnaire (e.g., Paper II-IV) in which the participants had to respond to predefined options. The received responses were later analyzed using statistical analysis procedures. Quantitative methods allow a more explicit interpretation of the research questions posed than qualitative methods. Both descriptive and inferential statistics were used for the statistical analysis. Besides, in Paper III, we applied a Confirmatory Factor Analysis (CFA) to perform a reliability and validity test of the measurements and a Structural Equation Modeling (SEM) to analyze the strength and directions along the paths between the constructs to analyze and test our hypotheses. For examining the internal reliability, and convergent and discriminant validity, we calculated Cronbach's alpha, composite reliability (Raykov's ω), and Average Variance Extracted (AVE), which are widely adopted measurements [31].

1.6 SUMMARY OF APPENDED PAPERS

Paper I: Do Privacy Concerns Prevent Employees' Acceptance of Smart Wearables and Collaborative Robots?

This paper categorizes related privacy research in smart workplaces based on a literature review and presents a set of research questions. The research questions consider, e.g., employees' knowledge and privacy concerns and describe the proceeding to address them in future research. The paper focuses on smart wearables and collaborative robots increasingly introduced due to the digitization of workplaces resulting in employees' privacy concerns.

Paper II: Exploration of Factors that can Impact the Willingness of Employees to Share Smart Watch Data with their Employers

This paper considers factors that may influence employees' willingness to share smart watch captured private data. Based on an online questionnaire, it analyzes the impacts of employees' legislation knowledge, technical knowledge about smart watch capabilities, and technical affinity on employees' willingness to share such information. It further shows that employees have partially incorrect knowledge about legal frameworks, especially about collective agreements and the GDPR purpose. Moreover, the results reveal that both the technical affinity and the ownership of a personal smart watch lead to differences in their willingness to share data. Based on the findings, we derive recommendations for employers.

Paper III: On the Impact of Information Provided to Employees on their Intention to Disclose Data Collected by Smart Watches to their Employers

This paper examines 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. The results show, that providing more information about both benefits and privacy risks side-by-side is not sufficient. Based on the findings, the paper shows that employers should be aware of this and provides adequate solutions for potential risks.

Paper IV: Enhanced Privacy in Smart Workplaces: Employees' Preferences for Transparency Indicators and Control Interactions in the Case of Data Collection with Smart Watches

Employees should be aware of any data collection and be able to control it. Therefore, this paper examines employees' preferences for different proposed privacy indicators to raise awareness about current data collection as well as interactions to stop this collection. Based on an online questionnaire, it shows that employees generally wish such awareness-raising indicators and control over data collection. Moreover, it shows that employees prefer familiar designs and interactions. Based on derived insights, we sug-

gest that employers should implement such mechanisms to benefit both employees and employers. Since employees benefit from more transparency and control, that could increase their trust in the employer and thus fostering their acceptance of smart workplaces.

Paper V: Privacy-Preserving Human-Machine Co-Existence on Smart Factory Shop Floors

This paper considers the co-existence of human workers and AGVs on smart factory shop floors and applies a privacy-preserving solution (spatial cloaking). The paper examines the AGVs' productivity and the resulting workers' safety through simulations when spatial cloaking is deployed to protect workers' location privacy transmitted with smart watches. The results show that larger cloaking radii improve workers' safety but this implies a significant reduction in the AGVs' productivity, which may not be compatible with a real-world deployment.

PAPER I

2

DO PRIVACY CONCERNS PREVENT EMPLOYEES' ACCEPTANCE OF SMART WEARABLES AND COLLABORATIVE ROBOTS?

ABSTRACT. During the digitization of workplaces, companies are increasingly using smart wearables as well as collaborative robots. This technological progress can contribute to higher productivity and efficiency in manufacturing processes, as they assist employees in carrying out their work. This changes the way employees interact and collaborate with their working environment and robots. When companies utilize smart wearables and collaborative robots in their processes, employees are exposed to various privacy issues, which may lead to privacy concerns and may reduce the acceptance of such devices and robots. Thus, the presented PhD research project aims to understand the employees' privacy concerns and address them.

KEYWORDS. Privacy · Employees' Acceptance · Smart Wearables · Collaborative Robots · Smart Workplaces

CITATION. A. Richter. Do Privacy Concerns Prevent Employees' Acceptance of Smart Wearables and Collaborative Robots?. Proceedings of the 10th Fachtagung Sicherheit, Schutz und Zuverlässigkeit (SICHERHEIT), 2020.

2.1 INTRODUCTION

Employees' work is changing in factories and other industries. Companies digitize manufacturing processes to optimize workplaces and operations to achieve higher productivity and greater efficiency. For this, smart wearables have the potential to contribute in increasing productivity. Therefore, an increasing number of companies are equipping their employees with smart wearables [15] to improve workers' productivity [17, 21], health [4, 6], and safety [2]. Another essential aspect in industrial processes is human-robot collaboration [11, 18], as humans and robots can collaborate in an increasing number of tasks due to a new generation of robots and sensors [11, 18]. However, to facilitate human-robot collaboration, the separation of their workspaces need to be eliminated [12, 18]. Therefore, different sensors to enhance employees' safety must be embedded in collaborative robots.

However, the potential benefits which entail from such devices and robots are always offset by risks that may affect the employees' privacy. For example, these risks arise from wearing such devices or the interaction with robots by the respective employee due to the possibilities to collect employees' data with the devices or robots. Various authors have already shown that the use of different sensors and devices enhance the possibility to endanger users' privacy [16, 20]. Examples include reading sensor data, such as the gyroscope or the acceleration sensor. These data make it possible to determine, i.e., users' physical activities. Equal potential risks are also able to arise in the corporate context. For example, this can be seen in the scandal of the Tesco company, where employees

were equipped with digital wristbands that allowed managers to find out how much the employees worked [1].

Both technologies are components of recent and future digitization of workplaces, as they can enhance productivity and employees' efficiency. Due to the embedded sensors, employers can collect, analyze, and draw inferences about the employees, especially, when they use them for entire shifts. Moreover, combining several sensors' data might give employers more insights regarding employees' sensitive data, for instance employees' health, job performance, etc. Therefore, this PhD research project examines the discrepancies between employers and employees, address them and potentially contribute to increase the acceptance of digitized processes. Thus, the main goal of the project is to first analyze whether the employees' privacy concerns influence their acceptance of such devices. Moreover, it aims to analyze whether increasing the data collection transparency control mechanisms, can improve employees' acceptance to mitigate such employees' concerns.

2.2 RELATED WORK

Previous research can be classified into three categories: (1) employees' acceptance, (2) privacy concerns, and (3) proposed solutions. The first category includes employees' acceptance surveys conducted in a corporate context, such as [2, 5, 7]. Choi, Hwang, and Lee identified different influence factors, like perceived usefulness, social influence, and perceived privacy risks, which have an impact on the adoption of smart wearables for occupational safety and health management. Beside employee beliefs, employees' acceptance can also be affected by job position in a company or experience with such devices [2, 5]. Existing work is mostly based on a specific use case. Jacobs et al. investigated factors that are related to the organizational settings, the individual employee, and the purpose or use case at the workplace.

In the second category, privacy concerns are identified and classified in different ways in existing works. These privacy concerns are closely related to the embedded sensors with the ability to sense, collect, and store data [9] and increase with a physical and temporal context [10]. Furthermore, users are not able to understand potential threats about collected data about behavior disclosures and context from measurements by sensors, unless these are their own data [10]. Besides, previous work mentioned general fears from employees in the context of workplace environments. These include the fear of being under surveillance or tracked by the employers [2, 3, 14] or the risk that the devices record sensitive information [2, 3]. This, especially with regard to surveillance and monitoring, may have a negative impact on job satisfaction and also in the level of employees' stress and may lead to a deterioration in productivity [8, 19].

For the latter category, different authors propose rules relevant to workplace surveillance [13] or offer recommendations to maximize the positive effects of electronic performance monitoring and to minimize negative ones [19]. These rules include several points such as informing the employees about the data that are collected or accessed as well as how employees can access and correct the information [13, 21]. Thus, employers should be transparent about monitoring processes and use the insights for learning and developing rather than for preventing unwanted employees' behavior. Moreover, employers should monitor only work-related behaviors [19]. Furthermore, employers must take reasonable measures to protect information from misuse, loss, unauthorized access, modification

or disclosure [13]. However, these are only general recommendations for employers. A general approach for employers to give employees the ability to gain access to gathered data to comply with the GDPR and thus to enhance employees' privacy is hence still missing.

To the best of our knowledge, there is no previous work that focuses on the following two issues: (1) analyzing employees' privacy concerns arising by the adoption of smart wearables or the collaboration with robots, based on their knowledge regarding possibilities of sensor readings as well as (2) developing an approach allowing employees to get more transparency and control over the collected data by wearables and robots especially w.r.t. the threats related to embedded sensors in smart workplaces. Therefore, our entire research work focuses on the above-mentioned issues.

2.3 RESEARCH QUESTIONS AND METHODOLOGY

The basis of the PhD research project relies on analyzing existing research papers, which address the key topics of smart workplaces, smart wearables, collaborative robots, control, transparency, and minimization of data as well as various technology acceptance models in the context of privacy.

In this work, we will analyze the impact of employees' privacy concerns on their acceptance to use smart wearables and collaborative robots as basis for the development of an approach to protect employees' privacy. In more detail, we will consider the following research questions.

Which privacy risks prevent the use of smart wearables or the collaboration with robots? — We will start by conducting, a structured literature review. Likewise, some in-depth case studies with helpful industry partners shall be conducted to get a closer look into processes with such devices and their implementation and use in companies. Core issues are risks and threats that may arise from these technologies and thus affect individuals' privacy. For a better understanding of existing privacy risks and threats, we will analyze and identify the general threats and risks of such devices, and the included sensors. Likewise, it includes sensors or techniques that threaten individuals' privacy.

Which employees' level of knowledge regarding privacy risks result in acceptance problems? — Regarding the previous insights, privacy concerns arising from employees' level of knowledge (knowledge or ignorance), need to be examined. Knowledge implies that employees are aware of risks for their privacy, which can result in the rejection of new technologies since they can understand the technology's data processing and occurring consequences. In comparison, ignorance implies that those rejection results from the fear based on a lack of knowledge about these potential risks towards their privacy, as they are not able to grasp how data collection or processing works or which consequences results from this data, for instance. Thus, these are two antagonistic causes from which privacy concerns may arise. For this purpose, a qualitative and quantitative survey shall contribute to identifying these concerns. Therefore, a first targeted and direct semi-structured interview with employees will be held and provide the first insights on perceived privacy risks and threats. Based on the qualitative interviews, a quantitative survey will be conducted that verifies the insights of the interviews and will confirm or reject their significance. For this purpose, the participants are presented with various benefit and risk scenarios, for

instance. From the conducted surveys, an analysis of the ensuing employees' acceptance problems is required about the use of those devices in the company context. For this purpose, the technology acceptance models such as Technology Acceptance Model (TAM) or Unified Theory of Acceptance and Use of Technology (UTAUT) will be analyzed and applied to the research problem.

Which information or conditions influence employees' acceptance? — By means of a survey, information and conditions shall be identified, which may positively influence the employees with respect to the adoption and use of smart wearables or the collaboration with robots. For this, it is necessary to verify, whether the control or transparency of the collected employees' data as well as the data minimization, e.g., by pseudonymization affects the deployment of these devices mentioned above. Therefore, it must be clarified to what extent to control, transparency, and data minimization are understandable in order to help the employers to respect the GDPR compliance and implement mechanisms to improve employees' privacy.

How do solutions need to be implemented in companies to ensure and enhance employees' privacy? — Based on the results obtained, an approach shall be formulated with the aim to improve employees' privacy. This can be achieved through control mechanisms and/or transparency of processes by the management but also through systems, which have already required to implement regarding the GDPR. However, companies need effective approaches to fulfill the requirements. Thereby, the employees' acceptance to use smart products could be enhanced. Afterwards, an evaluation of the proposed solution would take place by means of user studies.

2.4 SUMMARY AND EXPECTED CONTRIBUTIONS

This PhD research project aims to contribute in designing a model, e.g., an interface, that will enable employees to gain more transparency, access, and control over their personal information generated within the company, especially in presence of smart devices and collaborative robots. For companies to benefit from the above-mentioned advantages of the digitization of workplaces, our proposed approach could contribute to reduce employee's privacy concerns and consequently improve their acceptance.

REFERENCES

[1] S. A. Applin and M. D. Fischer. "Watching Me, Watching You. (Process Surveillance and Agency in the Workplace)." In: *Proc. of the 2013 IEEE International Symposium on Technology and Society (ISTAS): Social Implications of Wearable Computing and Augmediated Reality in Everyday Life*. 2013.

[2] B. Choi, S. Hwang, and S. H. Lee. "What drives Construction Workers' Acceptance of Wearable Technologies in the Workplace?: Indoor Localization and Wearable Health Devices for Occupational Safety and Health." In: *Automation in Construction* 84 (2017).

[3] P. Datta, A. S. Namin, and M. Chatterjee. "A Survey of Privacy Concerns in Wearable Devices." In: *Proc. of the IEEE International Conference on Big Data (Big Data)*. 2018.

[4] N. Gorm. "Personal Health Tracking Technologies in Practice." In: *Companion of the ACM Conference on Computer Supported Cooperative Work and Social Computing (CSCW)*. Ed. by C. P. Lee, S. Poltrock, L. Barkhuus, M. Borges, and W. Kellogg. 2017.

[5] J. V. Jacobs, L. J. Hettinger, Y.-H. Huang, S. Jeffries, M. F. Lesch, L. A. Simmons, S. K. Verma, and J. L. Willetts. "Employee Acceptance of Wearable Technology in the Workplace." In: *Applied Ergonomics* 78.1 (2019).

[6] E. Lingg, G. Leone, K. Spaulding, and R. B'Far. "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)*. 2014.

[7] V Lotz, S Himmel, and M Ziefle. "You're My Mate–Acceptance Factors for Human-Robot Collaboration in Industry." In: *Proc. of the International Conference on Competitive Manufacturing (COMA)*. 2019.

[8] N. Meyers. "Employee Privacy in the Electronic Workplace: Current Issues for IT Professionals." In: *Proc. of the 14th Australasian Conference on Information Systems (ACIS)*. 2003.

[9] V. G. Motti and K. Caine. "Users' Privacy Concerns About Wearables." In: *Proc. of the 18th International Conference on Financial Cryptography and Data Security (FC)*. Springer. 2015.

[10] A. Raij, A. Ghosh, S. Kumar, and M. Srivastava. "Privacy Risks Emerging from the Adoption of Innocuous Wearable Sensors in the Mobile Environment." In: *Proc. of the 29th ACM Conference on Human Factors in Computing Systems (CHI)*. 2011.

[11] S. Robla-Gómez, V. M. Becerra, J. R. Llata, E. Gonzalez-Sarabia, C. Torre-Ferrero, and J. Perez-Oria. "Working Together: A Review on Safe Human-Robot Collaboration in Industrial Environments." In: *IEEE Access* 5.1 (2017).

[12] D. Romero, J. Stahre, T. Wuest, O. Noran, P. Bernus, Fasth Fast-Berglund, and D. Gorecky. "Towards an Operator 4.0 Typology: A Human-Centric Perspective on the Fourth Industrial Revolution Technologies." In: *Proc. of the 46th International Conference on Computers and Industrial Engineering (CIE)*. 2016.

[13] G. A. Sandy. "Workplace Privacy and Surveillance: A Matter of Distributive Justice." In: *Proc. of the 17th Australasian Conference on Information Systems (ACIS)*. 2006.

[14] M. C. J. Schall, R. F. Sesek, and L. A. Cavuoto. "Barriers to the Adoption of Wearable Sensors in the Workplace: A Survey of Occupational Safety and Health Professionals." In: *Human Factors* 60.3 (2018).

[15] V. Schellewald, B. Weber, R. Ellegast, D. Friemert, and U. Hartmann. "Einsatz von Wearables zur Erfassung der körperlichen Aktivität am Arbeitsplatz." In: *DGUV Forum* 11 (2016).

[16] M. Shoaib, S. Bosch, H. Scholten, P. J. Havinga, and O. D. Incel. "Towards Detection of Bad Habits by Fusing Smartphone and Smartwatch Sensors." In: *Proc. of the 13th IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops)*. 2015.

[17] D. Spath, A. Weisbecker, M. Peissner, and C. Hipp. *Potenziale der Mensch-Technik Interaktion für die effiziente und vernetzte Produktion von morgen*. Stuttgart: Fraunhofer-Verlag, 2013. ISBN: 978-3-839-60563-9.

[18] J. J. Steil and G. W. Maier. "Robots in the Digitalized Workplace." In: *The Wiley Blackwell Handbook of the Psychology of the Internet at Work* (2017).

[19] D. L. Tomczak, L. A. Lanzo, and H. Aguinis. "Evidence-based Recommendations for Employee Performance Monitoring." In: *Business Horizons* 61.2 ().

[20] H. Wang, T. T.-T. Lai, and R. Roy Choudhury. "Mole: Motion Leaks Through Smartwatch Sensors." In: *Proc. of the 21st ACM Annual International Conference on Mobile Computing and Networking*. 2015.

[21] M. Weston. "Wearable Surveillance – A Step too far?" In: *Strategic HR Review* 14.6 (2015). ISSN: 1475-4398.

PAPER II

3

EXPLORATION OF FACTORS THAT CAN IMPACT THE WILLINGNESS OF EMPLOYEES TO SHARE SMART WATCH DATA WITH THEIR EMPLOYERS

ABSTRACT. Companies increasingly equip employees with smart watches to, e.g., support them in carrying out their work. Smart watches can however collect data about them and reveal sensitive information. This may result in limiting the acceptance of these devices by employees, despite their potential helpfulness. In this paper, we therefore analyze factors that influence employees' willingness to share smart watch captured private data. In more detail, we investigate employees' technological knowledge about data collection and processing and the associated risks, their technical affinity, their smart watch ownership and usage, and their legislation knowledge about respective laws. To this end, we have conducted an online survey with more than 1,000 full-time employees. Our findings suggest that employees are aware of the risk associated with smart watches but partially have incorrect knowledge about legal frameworks. Moreover, more than one-third of the participants own a personal smart watch and have a certain technological affinity. However, our results reveal different impacts from these factors on employees' willingness to share data with their employers.

KEYWORDS. Privacy · Employees · Willingness · Knowledge · Smart Watch

CITATION. A. Richter, P. Kühtreiber, D. Reinhardt. Exploration of Factors that can Impact the Willingness of Employees to Share Smart Watch Data with their Employers. Privacy and Identity Management. Between Data Protection and Security, 2022.

3.1 INTRODUCTION

An increasing number of smart wearables are sold worldwide and this trend is expected to continue in the next years [3]. Smart wearables are not only deployed for personal uses, but also in so-called smart workplaces. For example, companies seek to enhance their manufacturing processes and thus increase their productivity by using such devices [25, 29]. Among these smart wearables, smart watches can help support workers while they have their hands free for other tasks [16, 29, 37]. Similarly, they can lead to improvements in employees' health, if they encourage them to walk more [11]. For example, smart watches are already deployed in the BMW group. Employees in the production process wear smart watches which alert them when the next vehicle on the assembly chain has unusual requirements to remind them about the specifics of the next tasks to execute [2]. Other examples include Amazon and Tesco warehouses, in which such devices support employees in finding and collecting goods [6, 19]. While smart watches may offer several benefits, the collection and processing of data collected using their embedded sensors pose several risks to the wearers' privacy, as information about themselves and their environment can be obtained [1, 20]. Especially in this context, the devices have been used

to monitor employees' movement potentially, heart rate, daily number of steps, or their compliance to work process [1, 17]. This not only poses new challenges for employees' privacy, but can also be seen as a surveillance tool deployed by employers [17]. The resulting concerns may be amplified through the power imbalance between employees and employers, as employees usually cannot opt-out. However, they would likely choose to opt-out if they could [17]. In general, technical and legislation knowledge can be expected to influence users' privacy concerns or behaviors. For example, prior work suggest that knowledge about the collection and use of private data leads people to tend to be less concerned about their privacy [12, 22]. Likewise, legislation knowledge could help to reduce users' privacy concerns [23, 34]. Consequently, the lack of knowledge about technology and legislation would increase users' privacy concerns, thus negatively influence users' intention to disclose private data. This affect of privacy concerns on users' intentions was shown in different areas [9, 14, 32, 36]. However, other research also indicated that privacy awareness could lead to more privacy concerns [21, 24]. In this paper, our ultimate goal is the understanding of employees' willingness to share data with their employers by examining various factors that may impact it. Our contributions can be summarized as follows. We (1) investigate employees' understanding of data collection and processing, (2) their legislation knowledge, and finally, (3) the impact of both factors on employees' willingness to share smart watch data with their employers. To this end, we have conducted an online questionnaire answered by 1,214 participants. Our results show that employees are aware of smart watch risks. Moreover, their knowledge, especially about company agreements, is limited and even partially incorrect. Hence, both may cause additional privacy concerns and may lead to employees' rejection to share smart watch data with their employers. Our last contribution is to propose recommendations for employers when planning to introduce smart watches to their work processes.

In the remaining sections, we discuss related work in Sec. 3.2. We introduce our research goals in Sec. 3.3 and applied methodology in Sec. 3.4. We present our results in Sec. 3.5 with a focus on our hypotheses and discuss our results in Sec. 3.6. We further discuss our findings and recommendations in Sec. 3.7, before making concluding remarks in Sec. 3.8.

3.2 RELATED WORK

Existing studies focus on factors that may influence employees' acceptance to use smart wearables for various use cases [4, 13]. In [4], the focus is on construction workers' acceptance to use two different wearable technologies (smart vest, wristband) for occupational safety and health, while the focus is on use cases and work environments predicting employees' acceptance of wearables in [13]. As a result, both differ from our work, which focuses on smart watches and privacy-relevant aspects investigating employees' intention to disclose data to their employer rather than determine factors that influence the acceptance of wearable use. In both existing works, it is shown that the acceptance of smart wearables at work can be influenced by perceived privacy risks, or experiences with such devices, social influence and use cases. Consequently, both serve as an additional motivation for our work. In addition to these works, privacy concerns related to wearable devices in general have been discussed based on a literature review in [7], while multiple works, such as [8, 18, 26], show the feasibility of recognizing

the wearer's current activity based on the collected sensor data. Recommendations for employee performance monitoring systems have been further proposed in [31].

To the best of our knowledge, there exists no previous work investigating the impact of employees' knowledge about legislation and smart watches' data practices on their willingness to share these data with their employers.

3.3 RESEARCH GOALS

In our study, we aim at testing the following hypotheses:

- **H1:** Employees are more willing to share smart watch data with their employers depending on their smart watch ownership and usage.
- **H2:** Employees' willingness to share smart watch data with their employer is influenced by their knowledge about the capability of smart watches in terms of data collection and processing.
- **H3:** Employees' willingness to share smart watch data with their employer is influenced by their knowledge about legal frameworks.
- **H4:** Employees' willingness to share smart watch data with their employer is influenced by their technical affinity.

3.4 METHODOLOGY

3.4.1 *Survey Design*

To test our hypotheses, we have conducted a user study based on an online questionnaire. In addition to the participants' usage of smart watches, we have especially investigated their awareness about smart watches' capability regarding data collection and processing and their knowledge about legislation frameworks. To this end, we have provided a scenario to the participants (see Fig. 3.1), in which a deployment of smart watch was planned by their employer, after having collected their demographics to ensure a representative distribution across age and gender. In this scenario, we have detailed potential benefits along with information regarding data storage and a particular collected data type among activity, health, or location data.

We have then asked the participants about their intention to disclose this particular data type to their employer on a 5-point Likert scale from "strongly disagree" to "strongly agree" using three different questions derived from [30, 33, 35] (see Table 3.A.1 in Appendix 3.A).

Next, we have asked the participants whether they own a smart watch and to respectively provide information about their usage (see Table 3.A.2 in Appendix 3.A). Besides, we have asked them different questions about (1) smart watches' capability regarding data collection and processing (see Table 3.A.3 in Appendix 3.A) and (2) legislation frameworks (see Tables 3.A.4 and 3.A.5 in Appendix 3.A) in order to quantify their knowledge and understanding about both matters. We have finally evaluated their technical affinity using questions from [10] (see Table 3.A.6 in Appendix 3.A).

Your employer wants to conduct a study to test the use of smart watches in your company. Therefore, you have to wear this smart watch while performing your work.

The smart watch has an application that helps you perform your daily tasks.
Through the smartwatch, you can, for example:
- Access information faster and
- Request assistance if necessary.

- The smart watch does not have any applications other than that of your employer.
- To support you, different [**activity/health/location**] data needs to be collected.
- This information is stored centrally on the company's servers.

Figure 3.1: Provided scenario

3.4.2 *Survey Distribution*

Our study has been approved by the Data Protection Officer and the Ethic Committee of our university. Afterwards, it has been distributed by a panel certified ISO 26362. In total, 1,214 participants from Germany have answered our questionnaire in German. The participants have been evenly distributed among the three different data types, i.e., activity (395 participants), health (406), or location data (413). Using a confirmatory factory analysis, we have tested the measurement invariance that confirms a strong measurement invariance, meaning that the factors measure the same construct across all groups [15]. All our participants should be full-time employees working in Germany and over 18. Note that we have monetarily rewarded the participants' contributions.

3.4.3 *Survey Limitations*

The questionnaire first included additional aspects that we do not consider in this paper. Since the questions were disjoint and grouped in dedicated sections, their potential influence however remains limited. Second, our questionnaire is based on a hypothetical scenario that participants needed to imagine. As a result, they may not have fully connected the given scenario with their own work. This limitation is, however, shared with all other online questionnaire. Third, we focus on employees in Germany and over 18. The obtained results may be different for other cultures and employees younger than 18. We consider a cross-cultural study as a promising future work.

3.5 RESULTS

In this section, we detail the obtained results, while we specifically test our hypotheses formulated in Sec. 3.6.

3.5.1 *Demographics*

As shown in Table 3.1, our sample is evenly distributed between gender. The participants' age is between 18 and 67 years. Both distributions in terms of age and gender are

Table 3.1: Sample characteristics (N=1,214).

Levels		**Count**	**Percentage**
Gender	Female	590	48.6%
	Male	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%
Sector	Industry	189	15.6%
	Insurance	19	1.6%
	Business	57	4.7%
	IT	65	5.4%
	Health/social sector	168	13.8%
	Energy	19	1.6%
	Construction	70	5.8%
	Commerce	128	10.5%
	Traffic	69	5.7%
	Education, research, culture	93	7.7%
	Advertisement	17	1.4%
	Print	9	0.7%
	Social insurance	24	2.0%
	Bank/fiance	53	4.4%
	Not specified	234	19.3%
Occupational function	Worker	110	9.1%
	Employee	828	68.2%
	Team leader	92	7.6%
	Head of department	68	5.6%
	Division manager	33	2.7%
	Area manager	7	0.6%
	Manager	60	4.9%
	Not specified	16	1.3%

representative for the German population [28]. The majority are employees or workers (77.3%) working in industry (15.6%), the health/social sector (13.8%), or commerce (10.5%).

3.5.2 *Ownership and Usage*

In our sample, 35% use a smart watch in a private context. According to [27], 26% of Germans own smart watches, whereas our sample shows a slightly higher percentage of smart watch owners. Hence, those participants could be more ready to accept smart watches in other contexts than others, thus impacting their answers. We have considered this aspect in Section 3.6 in more detail. Many of them use it daily (73.4%). Although slightly more women (36.8%) than men (33.3%) stated that they own a smart watch, a Mann-Whitney U test shows that the gender does not significantly influence the smart watch ownership ($p = 0.209$). Among the participants younger than 55, the majority own a smart watch (66%). In comparison, only 38% of older participants own one. A Kruskal-Wallis test reveals a significant correlation between participants' age and smart watch ownership ($p < 0.05$). However, a pairwise comparison (Bonferroni corrected) shows significant differences between the age categories 18-24 and 55-67 ($p = 0.019$), 25-34 and 45-54, ($p = 0.010$), as well as 25-34 and 55-67 ($p = 0.005$).

3.5.3 *Technical Knowledge about Smart Watch Capabilities*

Our results show that many of our participants are aware of the technical capabilities of smart watches and the resulting threats to their privacy. Indeed, the participants are aware that a wide variety of profiles can be generated by combining individual personal data, such as a health profile (79.9%, Q_{TK1} in Table 3.A.3), and that these data can be used to draw inferences about their health (70.1%, Q_{TK2} in Table 3.A.3). In addition, a majority of the participants (61.6%, Q_{TK3} in Table 3.A.3) believe that the data collected with the help of a smart watch can be used to uniquely identify them. The same picture emerges for the total score of technical knowledge about smart watch capabilities whose results are displayed in Fig. 3.2. To evaluate the participants' knowledge, we have attributed a point for each correct answer to the questions Q_{TK1} to Q_{TK3}. A maximum of three points could be reached. For comparison purposes, we provide the results in percent. In the mean, participants' reached 71% of all points ($M = 2.12, SD = 1.00$). A Mann-Whitney U test shows that the results between women ($M = 2.03\ (67.7\%), SD = 1.00$) and men ($M = 2.20\ (73.3\%), SD = 1.00$) are significantly different ($p = 0.001$). No significant differences can however be identified between the different age categories.

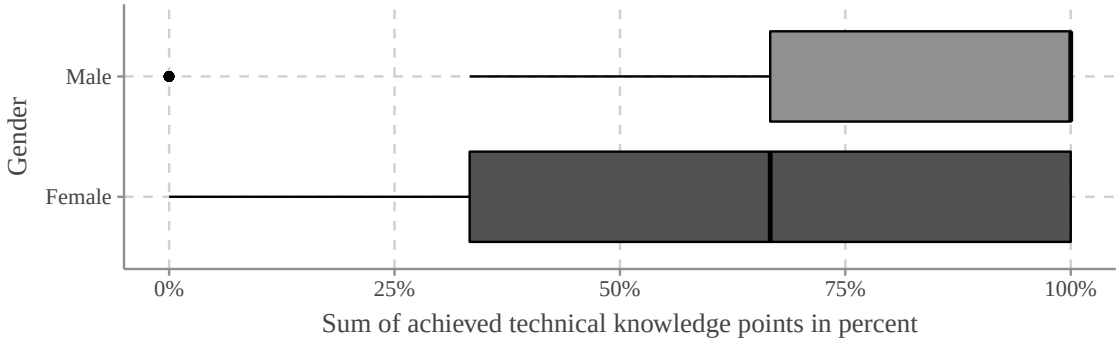


Figure 3.2: Participants' technical knowledge score about smart watch capabilities per gender

3.5.4 *Legislation Knowledge*

The participants' answers to the questions related to data protection regulations and laws in Germany and in a professional context shows that over half of the participants (55.8%) either do not know the GDPR purpose (23.8%) or have incorrect knowledge about it (31.8%, Q_{LK1} in Table 3.A.4). Note that our objective is not to blame our participants about it but to understand the current state to be able to improve it in the future. The other questions regarding GDPR reveal similar results. A half of the participants (52.1%) know what personal data are, while still some answered wrong (24.8%) or stated not to know (23.2%, Q_{LK2} in Table 3.A.4). Positively, the majority know when the processing of personal data is lawful (61.8%, Q_{LK3} in Table 3.A.4) or whereby consent to the collection of personal data occurs (60.7%, Q_{LK4} in Table 3.A.4). However, some respondents stated that they do not know (17.9%, Q_{LK3}/22.1%, Q_{LK4} in Table 3.A.4). A different picture emerges about the participants' knowledge of laws concerning the deletion of personal data. 35% indicated that deletion is required when the processing purpose and the legal retention period no longer apply. In contrast, 36.2% answered the opposite and 28.7% did not know (Q_{LK5} in Table 3.A.5).

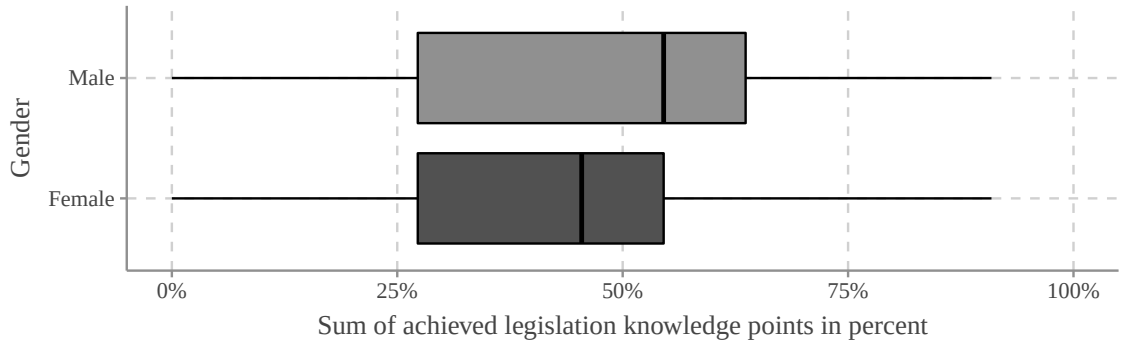


Figure 3.3: Participants' legislation knowledge score per gender

The lack of knowledge becomes particularly clear when it comes to collective agreements between employees and the employer. The majority of the participants (43.5%) indicated that collective agreements are not a permissible form of agreement to collect and use employees' data (Q_{LK6} in Table 3.A.5). In addition, some participants are not able to answer this question (31.9%). Similar results are obtained for the question of whether a collective agreement can replace the consent of a person (Q_{LK7} in Table 3.A.5). Here, only 21.1% know that a collective agreement can replace the consent of individuals. Only a few participants (38.4%) are even aware that employers are allowed to make collective agreements (Q_{LK8} in Table 3.A.5). 45.1% said they did not know. However, the majority (60.1%) knows that signing the employment contract does not create consent for collecting personal data for present and future purposes (Q_{LK9} in Table 3.A.5). In contrast, only 22.7% thought the opposite. Interestingly, however, most participants are aware that employers are allowed to measure employee performance (56.2%, Q_{LK10} in Table 3.A.5) and that at least the works council must be involved in the introduction and use of technical equipment designed to monitor employee behavior or performance (73.1%, Q_{LK11} in Table 3.A.5). When looking at the aggregated results displayed in Fig. 3.3 over the 11

questions (each correct answer corresponding to one point), an average of 44.6% of correct answers were achieved across all participants ($M = 4.91, SD = 2.23$). The results further indicate, that males reach significantly higher scores ($M = 5.05$ (45.9%), $SD = 2.26$) than females ($M = 4.76$ (43.3%), $SD = 2.19$) ($p = 0.019$, Mann-Whitney U test). Interestingly, overall females ($M = 3.24, SD = 3.04$) chose the option "I do not know" more frequently than males ($M = 2.48, SD = 2.96$, $p < 0.001$, Mann-Whitney U test). Significant differences are however not observed between age categories for both statements. In the following, we investigate differences in the legislation knowledge across occupational functions and sectors. Figure 3.4 shows differences in achieved legislation knowledge points between the specified functions, while Fig. 3.5 presents results between the sectors. A comparison of the means shows that workers ($M = 4.33$ (39.4%), $SD = 2.33$) achieved the lowest scores, while area managers achieved the highest ($M = 6.86$ (62.4%), $SD = 1.07$). The other positions achieved means between $M = 4.88$ (44.4%) to 5.25 (47.7%). Participants who did not specify their job function reached $M = 3.56$ (32.4%). Their answers reveal that the job function significantly impacts the legislation knowledge ($p = 0.006$, Kruskal-Wallis test). However, a pairwise comparison (Bonferroni corrected) indicates only a significant difference between "area managers" and those who did not specify their function.

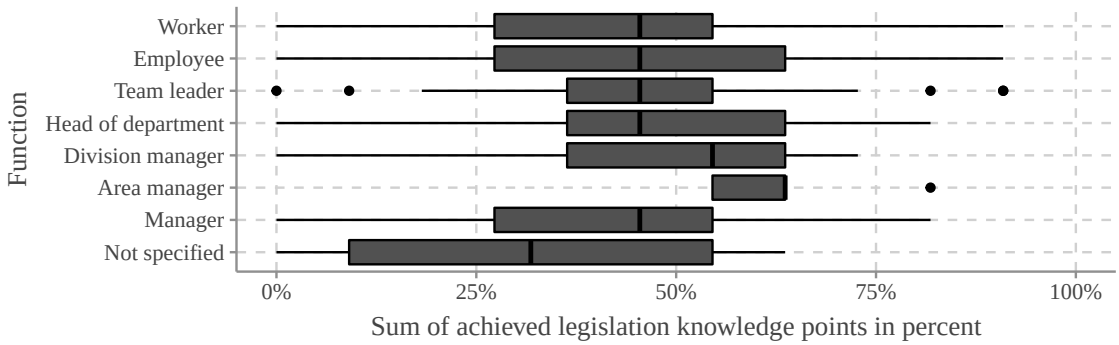


Figure 3.4: Participants' legislation knowledge score per function

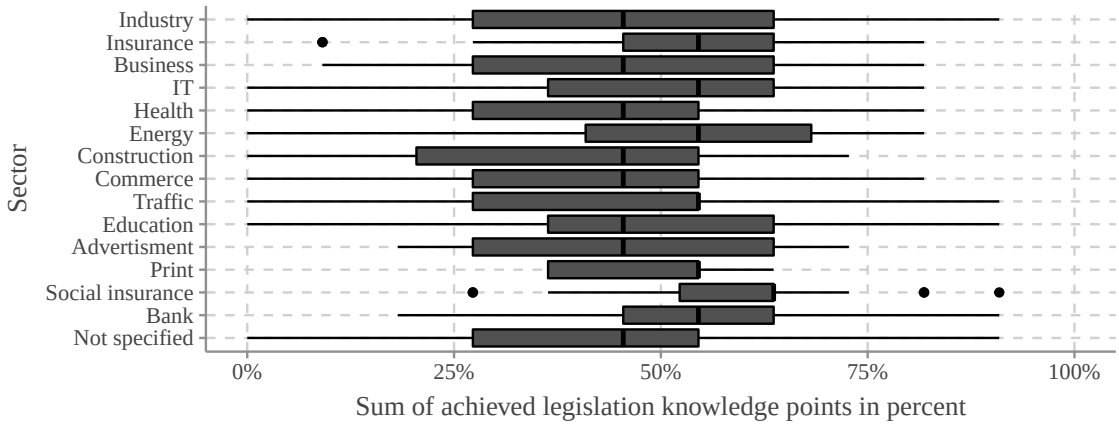


Figure 3.5: Participants' legislation knowledge score per sector

Regarding the sector, participants working in construction achieved the lowest mean with 4.30 (39.1%). While participants working in social insurance achieved the highest scores ($M = 5.94$ (54%), $SD = 1.75$). A Kruskal-Wallis test reveals that the sector impacts the legislation knowledge significantly ($p = 0.006$). However, a pairwise comparison (Bonferroni corrected) indicates significant differences only between the sectors construction to social insurance ($p = 0.003$) and bank ($p = 0.006$), between commerce and social insurance ($p = 0.037$), and between not specified and social insurance ($p = 0.002$) and bank ($p = 0.001$).

3.5.5 *Technical Affinity*

We apply the technical affinity scale proposed in [10] to classify our participants based on their technology affinity in order to understand its impact on the willingness to share private data with an employer. This scale contains nine questions. The affinity is determined based on the average of all answers indicated on a 6-point Likert scale. Hence, a total of six points can be achieved. The higher the value, the higher the participant's technical affinity. Overall, the mean score for all participants is 3.97 ($SD = 0.94$). The data displayed in Fig. 3.6 reveal that females ($M = 3.75, SD = 0.92$) reach significantly ($p = 0.001$) lower scores than males ($M = 4.17, SD = 0.91$). However, this effect is small ($r = 0.22$) [5]. When considering the different age categories, we observe a significant difference ($p = 0.028$). In detail, however, a pairwise comparison with Bonferoni correction shows that none of the groups significantly differ after correction.

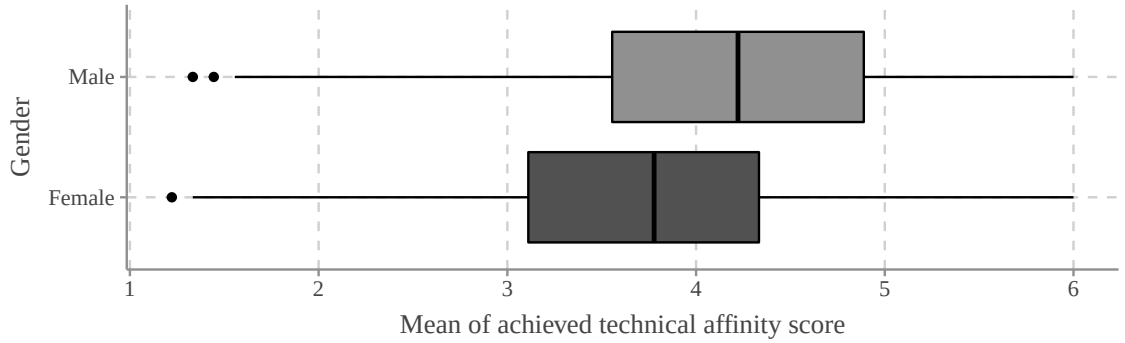


Figure 3.6: Participants' technical affinity score per gender

3.5.6 *Intention to Disclose*

We finally analyze the participants' intention to disclose the particular data type, i.e., activity, health, and location included in their respective scenario description, to their employer measured using the three questions presented in Table 3.A.1 in Section 3.A. A reliability analysis indicates excellent internal consistency across the answers provided to these three dedicated questions (Cronbach's $\alpha = 0.97$) [15]. As the participants are separated into three distinct groups based on the considered data type (activity, health, and location), we have further tested these groups for strict measurement invariance using a confirmatory factor analysis [15]. A strict measurement invariance requires equal latent

factor loadings, item intercepts, and residual and allows comparisons across groups as factors measure the same construct [15]. The test indicates no violation, meaning that the factors are measured identically across all groups, which allows meaningful comparisons.

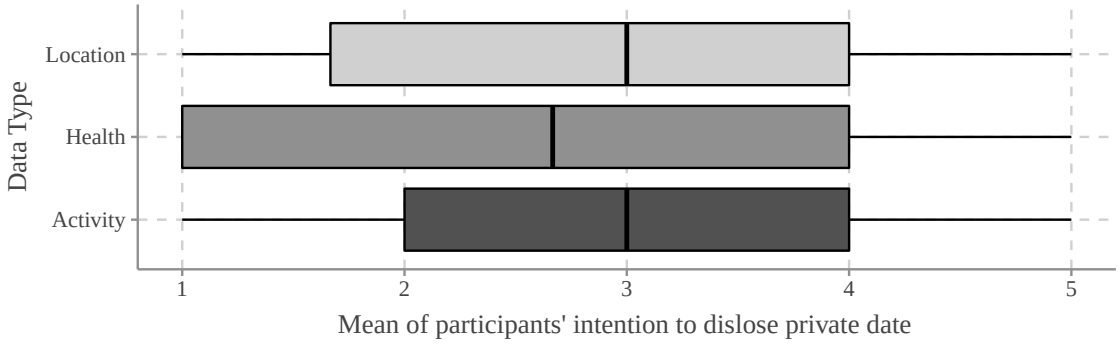


Figure 3.7: Means of participants' intention to disclose for each data type

Next, we have associated each item of the Likert scale to the corresponding point, i.e., 1 for "strongly disagree" and 5 for "strongly agree" and computed the mean over all three questions (Q_{ID1} to Q_{ID3} in Table 3.A.1) for each participant. With a mean of 2.82 ($SD = 1.36$), our participants are rather not willing to disclose the three data types to their employer. Neither age nor gender have any significant influence on their willingness. Concerning the different data types, a Kruskal-Wallis test shows that the data type has an impact on participants' intention to disclose it to their employer. Figure 3.7 presents and Table 3.2 summarizes the different results for each data type. A pairwise comparison (Bonferroni corrected) indicates that the participants are less willing to share their health data with their employer than their activity ($p = 0.001$) and their location ($p = 0.026$). There is no significant difference between location and activity.

Table 3.2: Data type mean overview

Type	N	M	SD	MIN	MAX	ΔActivity	ΔHealth
Activity	395	2.95	1.28	1	5	–	0.33
Health	406	2.63	1.37	1	5	−0.33	–
Location	413	2.88	1.39	1	5	−0.08	0.25
Total	1214	2.82	1.36	1	5		

3.6 TESTING THE HYPOTHESES

In the following, we test our hypotheses defined in Section 3.3 and discuss them with potential recommendations for employers.

H1: EMPLOYEES ARE MORE WILLING TO SHARE SMART WATCH DATA WITH THEIR EMPLOYERS DEPENDING ON THEIR SMART WATCH OWNERSHIP AND USAGE. As indicated in Section 3.5.2, more than one-third of the participants own a personal smart

watch and many of them use it on a daily basis. Our aforementioned results further confirm that especially younger people own a smart watch. In our hypothesis, we assume that employees who own and use their personal smart watch may be more willing to share the data with their employer due to their private experience and potential benefits drawn from it. The participants' answers confirm that participants who own a smart watch differ significantly from those who do not have a smart watch on their willingness to disclose the respective data type to their employers ($p < 0.001$, Mann-Whitney U test). In contrast, the differences regarding smart watch usage can be neglected, as a significant change cannot be observed. Thus, H1 is partially supported, as only participants who own a smart watch significantly differ in their willingness to share smart watch data with their employer compared to those who do not own a smartwatch.

In summary, the results in Section 3.5.2 reveal that one-third of participants from our sample own a smart watch, many of whom are younger participants. Furthermore, we found that participants who own a smart watch differ from those without a smart watch in their intention to disclose smart watch data to their employer, while no significant differences based on smart watch usage can be observed. Reasons for this may be that employees who own a smart watch tend to be more positive about data sharing, as they may be more tech-savvy and therefore better understand smart watch potentials, regardless of how often they ultimately use their smart watch. Based on this insight, employers could develop strategies. For example, they could provide employees a smart watch for private use before their introduction at the workplace. However, the professional and private usage should be strictly separated. Employers should not collect employees' data outside the company when it is not work-related [31]. This must be ensured as no legitimate reasons for such data collection exists unless employees have agreed. Beyond the implementation of such strategy, more and more people are buying smart watches for private use. This may lead to an increasing number of individuals becoming familiar with smart watches, thus resulting in more individuals willing to also use them in a corporate context. This trend is certainly related to the advantages that a smart watch can offer compared to the associated threats including to their privacy.

H2: EMPLOYEES' WILLINGNESS TO SHARE SMART WATCH DATA WITH THEIR EMPLOYER IS INFLUENCED BY THEIR KNOWLEDGE ABOUT THE CAPABILITY OF SMART WATCHES IN TERMS OF DATA COLLECTION AND PROCESSING. The obtained results for $Q_{TK1} - Q_{TK3}$ (Table 3.A.3 in Section 3.A) indicate good awareness about the technical capabilities of smart watches. Overall, most participants reach high scores. In particular, the results for Q_{TK1} and Q_{TK2} indicate that our participants are aware of smart watches being able to create health profiles, which allow deriving conclusions about the wearer. We hypothesize that the participants' technical knowledge about the capability of smart watches in terms of data collection and processing may influence their willingness to share those data with their employers. However, based on our data, neither significant positive nor negative influence is found between employees' technical knowledge about smart watches capabilities and employees' willingness to disclose data to their employers. Consequently, H2 is not supported.

However, to sum up, considering our findings in Section 3.5.3, our participants are already aware of the technical possibilities offered by a smart watch. We assume that this technological knowledge may negatively influence employees' decisions to accept a smart watch at work, even if we could not prove it in our study. Technical knowledge may

lead employees to negatively perceive the smart watch and the associated data collection, even if employers do not have bad intentions. In this case, providing transparency to the employees by explaining which data is being gathered, for which purpose, and how the data is protected is necessary. Besides, technical solutions to minimize potential risks for the employees should be implemented.

H3: EMPLOYEES' WILLINGNESS TO SHARE SMART WATCH DATA WITH THEIR EMPLOYER IS INFLUENCED BY THEIR KNOWLEDGE ABOUT LEGAL FRAMEWORKS. Although some participants already have partial knowledge about the GDPR, the lack of knowledge about collective agreements is shown in Section 3.5.4. At the same time, some participants are aware that employers are allowed to monitor employees' performance if the works council is involved. As a result, they may decide not to share their data with the employer. Therefore, we test our third hypothesis. The results reveal a significant positive relationship between employees' legislation knowledge and their willingness to share data with their employer ($p = 0.002$). The employees' disclosure intention increases by 0.053-unit ($+/-0.02$) for every increase in a unit of legislation knowledge. Thus, H3 is supported: The legislation knowledge influence employees' decision about smart watch data disclosure.

In summary, some of our participants have either no or even incorrect knowledge about the GDPR. Similarly, our participants are not aware of collective agreements that employers can negotiate and that those collective agreements can replace individual agreements. Interestingly, few participants are aware that employers are allowed to measure the employees' performance and that at least the works council has to be involved if technical equipment is used for such measurements. Overall, our participants thus achieved only low legislation knowledge scores. On top of that, we found that the influence from legislative knowledge on employees' willingness to share smart watch data with employers is positive, even if this influence is small. This positive influence may be explained by the fact that employees, who are aware that collective agreements are possible and that the works council should be included, feel more comfortable sharing data because the works council represents employees' interests and not those of the employer. Thus, employers should be aware that not every employee is aware of the collective agreements. Therefore, employers should clarify in advance the exact process from planning to integrating smart watches in their processes as well as which and where related information are available to employees. In addition, employers should generally agree on a code of conduct when dealing with employees' data to improve their trustworthiness and redress the prevailing imbalance between employers and employees. Furthermore, works councils should be sensitized to the issue so that they can fill potential knowledge gaps.

H4: EMPLOYEES' WILLINGNESS TO SHARE SMART WATCH DATA WITH THEIR EMPLOYER IS INFLUENCED BY THEIR TECHNICAL AFFINITY. The results in Section 3.5.5 indicate that our participants have a certain technological affinity. It can be assumed that participants with an affinity for technology are more willing to use a smart watch in a company, as they enjoy the use of new technologies. This may imply that it also applies to share their data with their employer. Based on the results derived from the regression model, employees' technical affinity impacts employees' willingness significantly ($p < 0.001$). This influence is positive, as for each increase unit in employees' technical

affinity employees' willingness to share smart watch data with their employer increase by 0.27-unit ($+/-0.04$). As a result, H4 is supported.

In short, in our sample, our participants exhibit a certain technological affinity, which positively influences employees' willingness to share smart watch data with employers. This impact may be positive as tech-savvy people tend to enjoy new technologies, which possibly implies the same in a corporate context and ultimately could foster data sharing. Nonetheless, employers could identify particularly tech-savvy employees to conduct prior studies with them to jointly identify potential barriers to later implementation and establish solutions.

In summary, our hypotheses H3 and H4 are confirmed, while H1 is partly confirmed and H2 is rejected.

3.7 DISCUSSION

Derived from our results presented in Sections 3.5 and 3.6, we highlight our following key insights and potential recommendations for employers. First, we found differences between participants who own a smart watch and those without a smart watch concerning their willingness to share data with the employer. With this in mind, employers could provide employees with smart watches for their private use before introducing them to workplace processes. A separation between private and corporate usage is beyond question and mandatory. Second, we found that our participants' knowledge about the GDPR is vague and partly incorrect. Moreover, there is a small positive influence on the willingness to share data with the employer when legislation knowledge increases. Employers should be aware of this and provide information, especially about collective agreements. They should also provide information in advance about the process of future implementation. More importantly, however, works councils should be sensitized to the issue to close any gaps in employees' knowledge when they exist.

In general, employers who decide to use smart watches in their processes should further analyze what data exactly needs to be collected. This is necessary for the employees' agreement allowing them to collect private data with a smart watch while working, which depends on the data type asked for. Our results show significant differences between the three considered types of data. Our participants were less willing to share health data with employers when compared to location and activity data. The difference between activity and health data is particularly interesting. They differ in the data collected due to the different sensors used. However, inferences about a wearer's health can be made even based on the wearer's activity. The participants might not be aware of this connection or might estimate that they are less likely. Employers should, therefore, analyze in advance exactly what data is relevant and why it should be collected. In principle, employers should always communicate with employees openly and transparently. This means that employers should provide clear information about what data is being collected and for what purpose. Implementing smart watches in workplaces requires careful planning and realization. The works council should always be included in this process if one exists. In the absence of a works council, employees should be actively involved in the implementation process. Moreover, companies should transparently report on the planned actions and provide suitable solutions for reducing employees' risks. In addition, technical solutions should be implemented to help employees enforce their rights. However, if there is strong opposition among the workforce towards smart watch

implementation and the associated data collection, employers should not exploit their position of power and refrain from using smart watches, even if all previous suggestions were considered.

3.8 CONCLUSIONS

In our study, we have explored factors that may influence employees' willingness to share data from smart watches with their employers. More precisely, we explored the impacts of employees' legislation knowledge, technical knowledge about smart watch capabilities, and technical affinity on their willingness to share such information. Moreover, we investigated whether the smart watch ownership and usage correlate with this willingness. A majority of our participants is aware of what can be processed and used with the data collected by a smart watch. Employees have, however, partially incorrect knowledge about legal frameworks, especially about collective agreements and the GDPR purpose. Moreover, our results reveal that the ownership of a personal smart watch leads to differences in their willingness to share data, as does the employees' technical affinity. Among the different data types considered, the participants were more reluctant to share health data. Thus, we recommend employers to consider employees' knowledge about smart watches and legislation frameworks when implementing smart watches to reduce potential misunderstandings about the data to be collected. Likewise, they should provide transparency about the collected data and apply adequate privacy-preserving mechanisms. While our results provide insights about factors, which impact employees' willingness to share data with their employer, the adopted scenarios remain general. As a result, we plan as a next step to conduct studies, such as interviews, which will take into account the specifics of the participants' work. Here, we will consider activity data more concretely. In addition, we will explore employees' trust in the GDPR in the future. Based on that, we further plan to develop methods to bridge potential employees' knowledge gaps and provide them both transparency and control over such data collection in the future.

ACKNOWLEDGMENTS

The authors would like to thank the anonymous participants who participated in the survey and our colleagues for their feedback on the survey.

REFERENCES

[1] S. A. Applin and M. D. Fischer. "Watching Me, Watching You.(Process Surveillance and Agency in the Workplace)." In: *Proc. of the IEEE International Symposium on Technology and Society (ISTAS): Social Implications of Wearable Computing and Augmediated Reality in Everyday Life*. 2013.

[2] BMW Group. *Produktionsstart der neuen BMW 7er Limousine*. 2019. URL: https://www.press.bmwgroup.com/austria/article/detail/T0292928DE (visited on 11/31/2021).

[3] CCS Insight. *Healthy Outlook for Wearables As Users Focus on Fitness and Well-Being*. 2021. URL: https://www.ccsinsight.com/press/company-news/healthy-outlook-for-wearables-as-users-focus-on-fitness-and-well-being/ (visited on 05/21/2021).

[4] B. Choi, S. Hwang, and S. H. Lee. "What Drives Construction Workers' Acceptance of Wearable Technologies in the Workplace?: Indoor Localization and Wearable Health Devices for Occupational Safety and Health." In: *Automation in Construction* 84.1 (2017).

[5] J. Cohen. *Statistical Power Analysis for the Behavioral Sciences*. Academic press, 1988.

[6] P. M. Collins and S. Marassi. "Is That Lawful?: Data Privacy and Fitness Trackers in the Workplace." In: *International Journal of Comparative Labour Law* 37.1 (2021).

[7] P. Datta, A. S. Namin, and M. Chatterjee. "A Survey of Privacy Concerns in Wearable Devices." In: *Proc. of the IEEE International Conference on Big Data (Big Data)*. 2018.

[8] A. Davoudi, A. A. Wanigatunga, M. Kheirkhahan, D. B. Corbett, T. Mendoza, M. Battula, S. Ranka, R. B. Fillingim, T. M. Manini, and P. Rashidi. "Accuracy of Samsung Gear S Smartwatch for Activity Recognition: Validation Study." In: *JMIR mHealth and uHealth* 7.2 (2019).

[9] T. Dinev and P. J. Hart. "An Extended Privacy Calculus Model for E-Commerce Transactions." In: *Information Systems Research* 17.1 (2006).

[10] T. Franke, C. Attig, and D. Wessel. "A Personal Resource for Technology Interaction: Development and Validation of the Affinity for Technology Interaction (Ati) Scale." In: *International Journal of Human–Computer Interaction* 35.6 (2019).

[11] N. Gorm and I. Shklovski. "Sharing Steps in the Workplace." In: *Proc. of the 34th ACM Conference on Human Factors in Computing Systems (CHI)*. 2016.

[12] J. Isaak and M. J. Hanna. "User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection." In: *Computer* 51.8 (2018).

[13] J. V. Jacobs, L. J. Hettinger, Y.-H. Huang, S. Jeffries, M. F. Lesch, L. A. Simmons, S. K. Verma, and J. L. Willetts. "Employee Acceptance of Wearable Technology in the Workplace." In: *Applied Ergonomics* 78.1 (2019).

[14] F. Kehr, T. Kowatsch, D. Wentzel, and E. Fleisch. "Blissfully Ignorant: The Effects of General Privacy Concerns, General Institutional Trust, and Affect in the Privacy Calculus." In: *Information Systems Journal* 25.6 (2015).

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

[16] K. Kovacs, F. Ansari, C. Geisert, E. Uhlmann, R. Glawar, and W. Sihn. "A Process Model for Enhancing Digital Assistance in Knowledge-Based Maintenance." In: *Machine Learning for Cyber Physical Systems*. 2019.

[17] M. Kritzler, M. Bäckman, A. Tenfält, and F. Michahelles. "Wearable Technology as a Solution for Workplace Safety." In: *Proc. of the 14th ACM International Conference on Mobile and Ubiquitous Multimedia (MUM)*.

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

[19] P. V. Moore. *The Quantified Self in Precarity: Work, Technology and What Counts*. 2017.

[20] V. G. Motti and K. Caine. "Users' Privacy Concerns About Wearables." In: *International Conference on Financial Cryptography and Data Security*.

[21] Z. D. Ozdemir, H. J. Smith, and J. H. Benamati. "Antecedents and Outcomes of Information Privacy Concerns in a Peer Context: An Exploratory Study." In: *European Journal of Information Systems* 26.6 (2017).

[22] C. Prince. "Do Consumers Want to Control Their Personal Data? Empirical Evidence." In: *International Journal of Human-Computer Studies* 110 (2018).

[23] C. Prince, N. Omrani, A. Maalaoui, M. Dabic, and S. Kraus. "Are We Living in Surveillance Societies and Is Privacy an Illusion? An Empirical Study on Privacy Literacy and Privacy Concerns." In: *IEEE Transactions on Engineering Management* (2021).

[24] F. Schaub, A. Marella, P. Kalvani, B. Ur, C. Pan, E. Forney, and L. F. Cranor. "Watching Them Watching Me: Browser Extensions' Impact on User Privacy Awareness and Concern." In: *Proc. of the Workshop on Usable Security (USEC)*. 2016.

[25] V. Schellewald, B. Weber, R. Ellegast, D. Friemert, and U. Hartmann. "Einsatz von Wearables zur Erfassung der körperlichen Aktivität am Arbeitsplatz." In: *DGUV Forum* 11.1 (2016).

[26] M. Shoaib, S. Bosch, H. Scholten, P. J. Havinga, and O. D. Incel. "Towards Detection of Bad Habits by Fusing Smartphone and Smartwatch Sensors." In: *Proc. of the 13th IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops)*. 2015.

[27] Statista Inc. *Do you personally use wearables (e.g. smart watch, health / fitness tracker)? [Graph]*. 2021. URL: `https://www.statista.com/forecasts/1101110/wearables-devices-usage-in-selected-countries` (visited on 11/31/2021).

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

[29] A. Stocker, P. Brandl, R. Michalczuk, and M. Rosenberger. "Mensch-zentrierte IKT-Lösungen in einer Smart Factory." In: *e & i Elektrotechnik und Informationstechnik* 131.7 (2014).

[30] Y. Sun, N. Wang, and S. X. "Perceived Benefits, Privacy Risks, and Perceived Justice in Location Information Disclosure: a Moderated Mediation Analysis." In: *Proc. of the Pacific Asia Conference on Information Systems (PACIS)*. 2014.

[31] D. L. Tomczak, L. A. Lanzo, and H. Aguinis. "Evidence-based Recommendations for Employee Performance Monitoring." In: *Business Horizons* 61.2 (2018).

[32] S. Trang and W. H. Weiger. "The Perils of Gamification: Does Engaging With Gamified Services Increase Users' Willingness to Disclose Personal Information?" In: *Comput. Hum. Behav.* 116 (2021).

[33] T. Wang, T. D. Duong, and C. C. Chen. "Intention to Disclose Personal Information via Mobile Applications: A Privacy Calculus Perspective." In: *International Journal of Information Management* 36.4 (2016).

[34] J. Wirtz, M. O. Lwin, and J. D. Williams. "Causes and Consequences of Consumer Online Privacy Concern." In: *International Journal of Service Industry Management* 18.4 (2007).

[35] H. Xu, H.-H. Teo, B. C. Tan, and R. Agarwal. "The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services." In: *Journal of management information systems* 26.3 (2009).

[36] X. Zhang, S. Liu, X. Chen, L. Wang, B. Gao, and Q. Zhu. "Health Information Privacy Concerns, Antecedents, and Information Disclosure Intention in Online Health Communities." In: *Information & Management* 55.4 (2018).

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

3.A APPENDIX: QUESTIONS

Table 3.A.1: Intention to disclosure

ID	Questions
Q_{ID1}	I am likely to share my information collected by the smart watch with my employer.
Q_{ID2}	I am probably going to be willing to share my information captured by the smart watch with my employer.
Q_{ID3}	I am certainly ready to be willing to share my information captured by the smart watch with my employer.

Possible answers: *5-point Likert scale from strongly disagree to strongly agree*

Table 3.A.2: Smart watch ownership and usage

ID	Questions
Q_{S1}	Do you own a smart watch that you use?

Possible answers: *Yes/No*

Q_{S2}	How often do you use your smart watch?

Possible answers: *Daily/Several times a week/Once a week/Less frequently*

Table 3.A.3: Technical knowledge about smart watch capabilities

ID	Questions
Q_{TK1}	Do you think that by combining individual personal data, it is possible to create a wide variety of profiles of you, such as a health profile or an activity profile?
Q_{TK2}	By capturing data collected with the help of a smart watch, for example, it is possible to identify them uniquely.
Q_{TK3}	The data collected with the help of a smart watch allows conclusions to be drawn about your state of health.

Possible answers: *Yes/No/I do not know*

Table 3.A.4: Legislation knowledge - part 1

ID	Questions
Q_{LK1}	What is the purpose of the General Data Protection Regulation (GDPR)?
A_{LK1}	*The GDPR regulates how any data collected exclusively via the Internet may be collected by companies.*
A_{LK2}	*The GDPR regulates how European citizens must provide their personal data to companies.*
A_{LK3}	*The GDPR regulates how companies may maintain and use the integrity of personal data.*
A_{LK4}	*The GDPR regulates how companies from non-EU countries may contact you.*
A_{LK5}	*I do not know*
Q_{LK2}	According to the GDPR, personal data are...
A_{LK1}	*...any information relating to an identified or identifiable natural person.*
A_{LK2}	*...all online information relating to an identified or identifiable natural person.*
A_{LK3}	*...all online information that relates to an identified or identifiable legal entity.*
A_{LK4}	*...all information relating to an identified or identifiable legal entity.*
A_{LK5}	*I do not know*
Q_{LK3}	The processing of personal data is lawful if...
A_{LK1}	*...a company clearly explains and demonstrates the purpose of the collection.*
A_{LK2}	*...the processing is absolutely necessary for the purpose of using a service.*
A_{LK3}	*...the data subject has given consent to processing for a specific purpose.*
A_{LK4}	*...the data subject is granted the right to erasure.*
A_{LK5}	*I do not know*
Q_{LK4}	Consent to the collection of personal data takes place,...
A_{LK1}	*...already when the person concerned is inactive or silent.*
A_{LK2}	*...even if a company does not ask you directly, but a service is used.*
A_{LK3}	*...if the consent is given by a clear confirming action for a specific purpose.*
A_{LK4}	*...already when you call up a company website.*
A_{LK5}	*I do not know*

Table 3.A.5: Legislation knowledge - part 2

ID	Questions
Q_{LK5}	According to the GDPR, personal data must be deleted if...
A_{LK1}	*... the data subject changes to another provider of a service.*
A_{LK2}	*... the purpose of the processing as well as the legal retention period ceases to apply.*
A_{LK3}	*... the purpose of the processing, regardless of the legal retention period, no longer applies.*
A_{LK4}	*... the data subject has requested information about the data, the data will subsequently be deleted.*
A_{LK5}	*I do not know*
Q_{LK6}	A collective agreement between employees and the employer can replace the consent of an individual.
Q_{LK7}	Collective agreements between employers and employees, constitute a permissible form of agreement to collect and use personal data of employees.
Q_{LK8}	Employers are permitted to conclude collective agreements (e.g., collective bargaining agreements) within the meaning of the German Federal Data Protection Act (BDSG).
Q_{LK9}	Signing your employment contract creates consent for any purposes of collecting personal data for present and future.
Q_{LK10}	Companies are generally prohibited from measuring employee performance.
Q_{LK11}	The works council must be involved in the introduction and use of technical equipment designed to monitor the behavior or performance of employees.

Possible answers: *True/Not true/I do not know*

Table 3.A.6: Affinity for technology interaction [10]

ID	Questions
Q_{ATI1}	I like to occupy myself in greater detail with technical systems.
Q_{ATI2}	I like testing the functions of new technical systems.
Q_{ATI3}	I predominantly deal with technical systems because I have to.
Q_{ATI4}	When I have a new technical system in front of me, I try it out intensively.
Q_{ATI5}	I enjoy spending time becoming acquainted with a new technical system.
Q_{ATI6}	It is enough for me that a technical system works; I don't care how or why.
Q_{ATI7}	I try to understand how a technical system exactly works.
Q_{ATI8}	It is enough for me to know the basic functions of a technical system.
Q_{ATI9}	I try to make full use of the capabilities of a technical system.

Possible answers: *6-point Likert scale from completely disagree to completely agree*

PAPER III

4

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

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 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

CITATION. A. Richter, P. Kühtreiber, D. 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.

4.1 INTRODUCTION

An increasing number of employers are relying on information technologies to monitor their employees [15]. As a result, they gather data about their employees from different sources to investigate, e.g., attitudes and monitor the performance [7]. 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 [43]. Employees can benefit from smart watches due to their unique characteristics [2]. 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 [67, 68]. Moreover, smart watch embedded sensors can promote employees' health [42] or increase occupational safety [14]. However, smart watches can determine and track wearers' location [20] or even recognize current activity based on sensor data [17, 46]. Therefore, employers can use smart watch data to check whether the employees are at their workplace [54], track their smoking behavior [55], or infer the employees' general health [51] and emotions [58]. Furthermore, smart watches are usually continuously worn, while a smartphone and other information systems are not [12]. 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 [48, 59], 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 [52, 60] and often ignored [44]. Additionally, employees may underestimate the privacy risks resulting from the smart watches, which leads to a lack of awareness and knowledge [52]. 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 [7]. This, in turn, usually requires employees' acceptance to use such devices, which benefits both employers and employees [31], 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 [27]. 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 [59, 64], 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 Section 4.2, we discuss the theoretical background, before presenting our research model in Section 4.3. We detail our methodology in Section 4.4 applied in our scenario-based online study. In Section 4.5, we present the respective results and discuss our findings in Section 4.6, before making concluding remarks in Section 4.7.

4.2 THEORETICAL FOUNDATION AND RELATED RESEARCH

Privacy calculus: Several models were used to explain new technology acceptance, like the *TAM* [29, 36]. However, these neither consider the impact of user privacy attitudes [52] 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 [62]. Privacy is described by Westin [63] 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 *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 [4]. However, whereas the trade-off in CPM theory is associated with disclosure in interpersonal situations [50], the trade-off in the privacy calculus model is related to the disclosure of information to an organization [4]. The privacy calculus was initially developed as the "calculus of behavior" by Laufer and Wolfe [39] 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 [16] 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 [18, 40]. 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 [18]. In contrast, potential benefits are monetary rewards, personalization [56], or locatability [66]. 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 [65]. Perceived surveillance, however, increased the privacy concerns [13], which shows that transparency of data usage is paramount. Privacy calculus has also been conceptualized [33] and confirmed [32, 40] as the basis for decision making in the context of wearables for, e.g., health purposes. Li et al. [40], 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 [49]. The privacy calculus model has also been used in the context of employees' privacy [11]

and to investigate employees' acceptance of a smart emergency detection system based on employees' tracking [52]. Apart from using the privacy calculus, other authors have already considered privacy in their studies. Regarding the workplace setting, Schall, Sesek, and Cavuoto [53] 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 deployment of electronic performance monitoring to reduce potential negative effects while increasing the positive ones [59, 64]. According to the rules, employees should be informed about data collected or accessed and their options to access and correct that information [64]. 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 [59]. 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 [1]. 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 [1]. 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 [1], 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 [40]. 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.

4.3 RESEARCH MODEL AND HYPOTHESES

To answer the research questions from Section 4.1, we propose a research model (see. Fig. 4.3.1) and describe our research model's used constructs and corresponding hypotheses in more detail in the following for each construct.

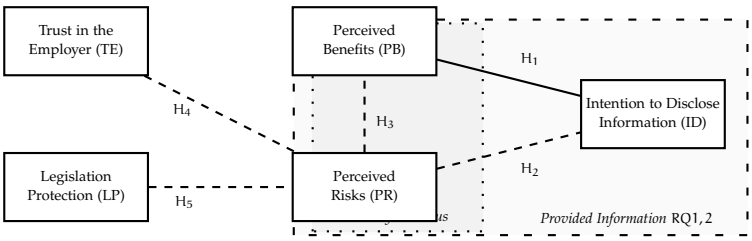


Figure 4.3.1: Research model

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 the enhancement of the job performance [14] or reflects the benefits that a user gains when utilizing such systems [41]. 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 [34, 64] 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 [58]. 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 [43, 58], the detection of work-related stress and fatigue [43, 47], or the improvement of employees' safety in case of hazardous situations using warning signals [14, 43]. 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 [35, 47]. 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 [47]. Wearable devices employed in that manner may harm employees' privacy and represent a new level in monitoring and control. Likewise, Tirabeni [58] 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 [58]. 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 [6], for example, as they often do not understand what the consequences of such disclosures can be [24]. 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 [14]. 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 [25]. 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" [38] 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 [4]. 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 [4]. Likewise, research in the context of self-disclosure online suggests that users' trust in a company affects their willingness to disclose more information online [9, 21]. In a work-related context, trust in the employer is also crucial in employees' readiness to accept being monitored by various sensors [52]. 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 [52]. 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 [3]. Besides, trust is also negatively affected by the perceived amount of data tracking in the workplace [10]. This can also be seen when data collected is used to punish them [23]. Despite that, Princi and Krämer [52] 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 [45, 52]. 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 [41]. 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 [19, 40]. 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 [19, 56]. 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 *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 *BDSG* to supplement, concretize, and specify these requirements. Besides, the *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

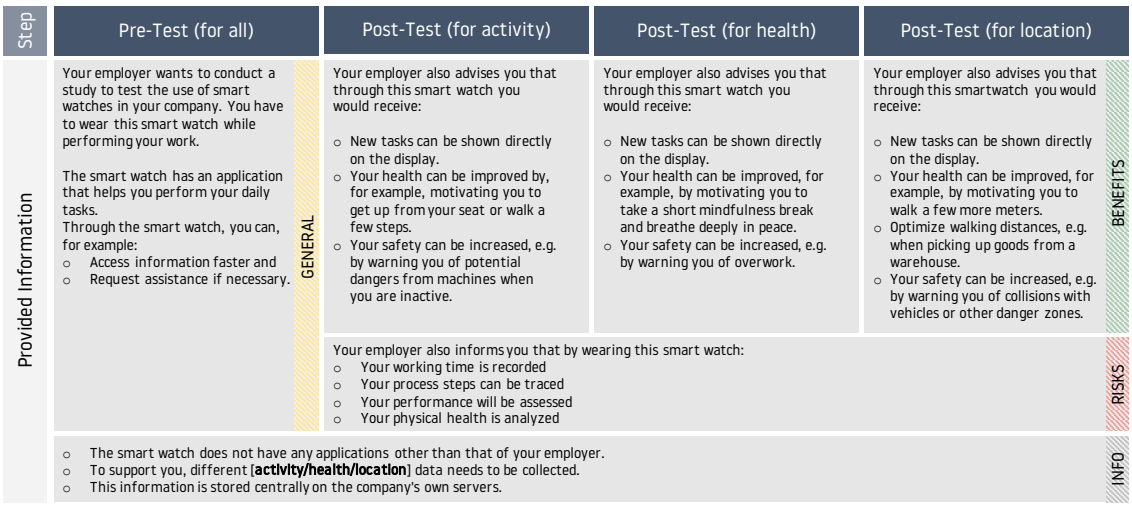


Figure 4.4.1: Overview of provided information in the given scenario

protection [19, 40, 66]. Xu et al. [66] examined the negative impact of privacy-related intervention in governmental regulations in location-based services. Likewise, Dinev et al. [19] demonstrated that regulatory expectations could effectively reduce individuals' perceived risk as a predictor of perceived privacy. Further, Li et al. [40] 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.

4.4 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 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. 4.4.1, while Section 4.4 provides an overview of the constructs' used items. For all

Constructs	Measurement items	Source
Intention to Disclosure (ID)	ID1: I am likely to disclose my *activity, health, location* information by using a smart watch ID2: I am willing to disclose my *activity, health, location* information by using a smart watch ID3: I am definitely willing to share my *activity, health, location* captured by the smart watch with my employer	[5, 61, 66]
Perceived Benefits (PB)	PB1: I believe that using a smart watch would improve my *health* in doing my job PB2: I believe that using a smart watch would improve my *safety* in doing my job PB3: I believe that using a smart watch would increases my *productivity* in doing my job	[14, 36, 40]
Perceived Risks (PR)	PR1: I believe that it would be risky to disclose my personal information to my employer PR2: I believe that there would be high potential for loss associated with disclosing my personal information to my employer PR3: I believe that there would be too much uncertainty associated with giving my personal information to my employer	[40]
Legislative Protection (LP)	LP1: I believe that the law should protect me from the misuse of my personal data by my employer LP2: I believe that the law should govern and interpret the practice of how my employer collect, use, and protect my private information LP3: I believe that the law should be able to address violation of the information I provided to my employer	[19]
Trust in the Employer (TE)	TE1: I believe that my employer handle my personal information confidentially TE2: I believe that my employer handle my personal information correctly TE3: I believe that my employer are always honest to me about how they use my personal information TE4: I believe that my employer protect my personal information I share with them	[9, 52]

Table 4.4.1: Constructs and measurement items

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. 4.4.1. 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. 4.3.1.

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 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 [57]. 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). Section 4.4 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 4.4.2: Sample characteristics (N= 1,214).

Data analyses: A *CFA* was used on the collected data to perform a reliability and validity test of the measurements and a *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 [37, p. 77], as the normal distribution assumption was violated for some items. For all models, gender and age were controlled. Section 4.4 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 ω), and *AVE*, which are widely used measurements [22]. Table 4.4.3 summarizes recommended (according to [26, 28]) 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 [37, 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.

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

Construct	mean	sd	α	ω	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 4.4.3: Descriptive statistics, reliability and correlations of measured constructs

compare the changes after the post-test.

Measurement model: The measurements displayed in Table 4.4.3 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 [30]. 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 Table 4.4.3, indicating acceptable discriminant validity [8, 22]. In addition, the CFA fit indices for the measurement model showed acceptable results compared to minimum values recommended in prior studies (see Table 4.5.1) [26, 28].

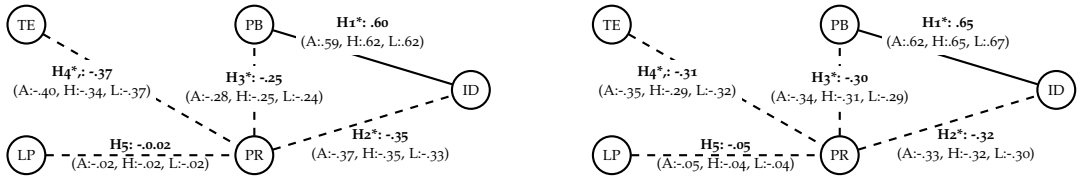
Structural model: The SEM results presented in Table 4.5.1 indicate also acceptable model fit indices based on recommended thresholds [28]. The SEM revealed that for all proposed paths, except for path LP $\rightarrow$ PR (**H5**, $\beta = -0.02$, $p = 0.72$), the standard coefficients β were significant. 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**, $\beta = 0.56$).

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 4.5.1: Fit indices of measurement and structural model

Measured impacts: The characteristics of the descriptive values for the main constructs (see Table 4.4.3) 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



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

Figure 4.5.1: Results along the paths for both provided information conditions with negative (dashed) and positive (solid) effects

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 ($M = 3.17$, $SD = 1.17$) 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. 4.5.1). 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 ($\beta_\Delta + 0.05$).

4.6 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.

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 4.6.1: Summary of the hypothesis tests

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 [14, 40] 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 [14, 40]. 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 [52]. 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 [21]. However, this cannot always

be assumed in an employment relationship. This is shown by results of Princi and Krämer [52], 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 [66] or wearable devices in health care [40]. 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 Section 4.5 and depicted in Fig. 4.5.1 revealed the changes from Fig. 4.5.1a to Fig. 4.5.1b. 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.

4.7 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

[1] I. Adjerid, A. Acquisti, L. Brandimarte, and G. Loewenstein. "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. 2013.

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

[3] M. Allen, S. J. Coopman, J. L. Hart, and K. L. Walker. "Workplace Surveillance and Managing Privacy Boundaries." In: *Management Communication Quarterly* 21.2 (2007).

[4] C. Anderson and R. Agarwal. "The Digitization of Healthcare: Boundary Risks, Emotion, and Consumer Willingness to Disclose Personal Health Information." In: *Information Systems Research* 22.3 (2011).

[5] G Bansal. "The Impact of Personal Dispositions on Information Sensitivity, Privacy Concern and Trust in Disclosing Health Information Online." In: *Decision Support Systems* 49.2 (2010).

[6] J. Barata and P. R. da Cunha. "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)*. 2019.

[7] D. P. Bhave, L. H. Teo, and R. S. Dalal. "Privacy at Work: A Review and a Research Agenda for a Contested Terrain." In: *Journal of Management* 46.1 (2020).

[8] G.-W. Bock, R. W. Zmud, Y.-G. Kim, and J.-N. Lee. "Behavioral Intention Formation in Knowledge Sharing: Examining the Roles of Extrinsic Motivators, Social-Psychological Forces, and Organizational Climate." In: *MIS Quarterly* 29.1 (2005).

[9] N. Bol, T. Dienlin, S. Kruikemeier, M. Sax, S. C. Boerman, J. Strycharz, N. Helberger, and C. H. De Vreese. "Understanding the Effects of Personalization as a Privacy Calculus: Analyzing Self-Disclosure Across Health, News, and Commerce Contexts." In: *Journal of Computer-Mediated Communication* 23.6 (2018).

[10] S. E. Change, A. Y. Liu, and Y.-T. J. Jang. "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)*. 2017.

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

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

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

[14] B. Choi, S. Hwang, and S. H. Lee. "What Drives Construction Workers' Acceptance of Wearable Technologies in the Workplace?: Indoor Localization and Wearable Health Devices for Occupational Safety and Health." In: *Automation in Construction* 84.1 (2017).

[15] P. M. Collins and S. Marassi. "Is That Lawful?: Data Privacy and Fitness Trackers in the Workplace." In: *International Journal of Comparative Labour Law* 37.1 (2021).

[16] M. J. Culnan and P. K. Armstrong. "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation." In: *Organization science* 10.1 (1999).

[17] A. Davoudi, A. A. Wanigatunga, M. Kheirkhahan, D. B. Corbett, T. Mendoza, M. Battula, S. Ranka, R. B. Fillingim, T. M. Manini, and P. Rashidi. "Accuracy of Samsung Gear S Smartwatch for Activity Recognition: Validation Study." In: *JMIR mHealth and uHealth* 7.2 (2019).

[18] T. Dinev and P. J. Hart. "An Extended Privacy Calculus Model for E-Commerce Transactions." In: *Information Systems Research* 17.1 (2006).

[19] T. Dinev, H. Xu, J. H. Smith, and P. Hart. "Information Privacy and Correlates: An Empirical Attempt to Bridge and Distinguish Privacy-Related Concepts." In: *European Journal of Information Systems* 22.3 (2013).

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

[21] R. Fletcher and S. Park. "The Impact of Trust in the News Media on Online News Consumption and Participation." In: *Digital journalism* 5.10 (2017).

[22] C. Fornell and D. F. Larcker. "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error." In: *Journal of Marketing Research* 18.1 (1981).

[23] J. F. George. "Computer-Based Monitoring: Common Perceptions and Empirical Results." In: *MIS Quarterly* (1996).

[24] N. Gorm and I. Shklovski. "Sharing Steps in the Workplace." In: *Proc. of the 34th ACM Conference on Human Factors in Computing Systems (CHI)*. 2016.

[25] J. Häikiö, J. Kallio, S.-M. Mäkelä, and J. Keränen. "Iot-Based Safety Monitoring From the Perspective of Construction Site Workers." In: *International Journal of Occupational and Environmental Safety* 4.1 (2020).

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

[27] S. Hobert and M. Schumann. "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)*. 2018.

[28] L.-t. Hu and P. M. Bentler. "Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives." In: *Structural equation modeling: a multidisciplinary journal* 6.1 (1999).

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

[30] C. Huang, Y. Wang, T. Wu, and P. Wang. "An Empirical Analysis of the Antecedents and Performance Consequences of Using the Moodle Platform." In: *International Journal of Information and Education Technology* 3.2 (2013).

[31] J. V. Jacobs, L. J. Hettinger, Y.-H. Huang, S. Jeffries, M. F. Lesch, L. A. Simmons, S. K. Verma, and J. L. Willetts. "Employee Acceptance of Wearable Technology in the Workplace." In: *Applied Ergonomics* 78.1 (2019).

[32] T. Jernejcic and O. El-Gayar. "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)*. 2021.

[33] N. von Kalckreuth and M. A. Feufel. "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)*. 2021.

[34] J. Khakurel, H. Melkas, and J. Porras. "Tapping Into the Wearable Device Revolution in the Work Environment: A Systematic Review." In: *Information Technology & People* 31.3 (2018).

[35] J. Khakurel, S. Pöysä, and J. Porras. "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)*. 2016.

[36] K. J. Kim and D.-H. Shin. "An Acceptance Model for Smart Watches: Implications for the Adoption of Future Wearable Technology." In: *Internet Research* 25.4 (2015).

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

[38] M. Korczynski. "The Political Economy of Trust." In: *Journal of Management Studies* 37.1 (2000).

[39] R. S. Laufer and M. Wolfe. "Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory." In: *Journal of social Issues* 33.3 (1977).

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

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

[42] E. Lingg, G. Leone, K. Spaulding, and R. B'Far. "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)*. 2014.

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

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

[45] D. H. McKnight and N. L. Chervany. "What Trust Means in E-Commerce Customer Relationships: An Interdisciplinary Conceptual Typology." In: *International journal of electronic commerce* 6.2 (2001).

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

[47] T. Mettler and J. Wulf. "Physiolytics at the Workplace: Affordances and Constraints of Wearables Use From an Employee's Perspective." In: *Information Systems Journal* 29.1 (2019).

[48] N. Meyers. "Employee Privacy in the Electronic Workplace: Current Issues for IT Professionals." In: *Proc. of the 14th Australasian Conference on Information Systems (ACIS)*. 2003.

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

[50] S. Petronio. *Boundaries of Privacy: Dialectics of Disclosure*. 2002.

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

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

[53] M. C. J. Schall, R. F. Sesek, and L. A. Cavuoto. "Barriers to the Adoption of Wearable Sensors in the Workplace: A Survey of Occupational Safety and Health Professionals." In: *Human Factors* 60.3 (2018).

[54] S. Sen, K. K. Rachuri, A. Mukherji, and A. Misra. "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)*. 2016.

[55] M. Shoaib, S. Bosch, H. Scholten, P. J. M. Havinga, and O. D. Incel. "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)*. 2015.

[56] H. J. Smith, T. Dinev, and H. Xu. "Information Privacy Research: An Interdisciplinary Review." In: *MIS quarterly* (2011).

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

[58] L. Tirabeni. "Technology, Power, and the Organization: Wearable Technologies and Their Implications for the Performance Appraisal." In: *Performance Appraisal in Modern Employment Relations*. 2020.

[59] D. L. Tomczak, L. A. Lanzo, and H. Aguinis. "Evidence-based Recommendations for Employee Performance Monitoring." In: *Business Horizons* 61.2 (2018).

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

[61] T. Wang, T. D. Duong, and C. C. Chen. "Intention to Disclose Personal Information via Mobile Applications: A Privacy Calculus Perspective." In: *International Journal of Information Management* 36.4 (2016).

[62] A. Weinhard, M. Hauser, and F. Thiesse. "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)*. 2017.

[63] A. F. Westin. *Privacy and Freedom*. Atheneum, 1967.

[64] M. Weston. "Wearable Surveillance – a Step Too Far?" In: *Strategic HR Review* 14.6 (2015).

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

[66] H. Xu, H.-H. Teo, B. C. Tan, and R. Agarwal. "The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services." In: *Journal of management information systems* 26.3 (2009).

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

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

PAPER IV

5

ENHANCED PRIVACY IN SMART WORKPLACES: EMPLOYEES' PREFERENCES FOR TRANSPARENCY INDICATORS AND CONTROL INTERACTIONS IN THE CASE OF DATA COLLECTION WITH SMART WATCHES

ABSTRACT. Employees are increasingly wearing smart watches for their work duties. While these devices can support employees in their tasks, they can also collect sensitive information like health or location data about them, thus endangering their privacy. Even when collective agreements, allowing employers to collect such data have been signed, we argue that employees should be aware of the data collection and be able to control it. Therefore, we propose different indicators that aim at enhancing employees' awareness about the current data collection as well as interactions to allow them to stop and resume it according to their preferences. To compare them, we have conducted an online questionnaire-based study with 1,033 participants. The results indicate that our participants wish to have such indicators to raise their awareness and further wish to control the data collection.

KEYWORDS. Smart Workplaces · Smart Watches · Privacy Awareness · Privacy Indicators · Control Mechanisms · Preferences

CITATION. A. Richter, P. Kühtreiber, D. Reinhardt. Enhanced Privacy in Smart Workplaces: Employees' Preferences for Transparency Indicators and Control Interactions in the Case of Data Collection with Smart Watches. Proceedings of the 37th International Conference on ICT Systems Security and Privacy Protection (IFIP SEC), 2022.

5.1 INTRODUCTION

More and more smart watches are sold worldwide [6, 15]. In addition to be used for private purposes, companies also recognize their potential and increasingly equip their employees with such devices [20, 42]. For example, they are used for allowing faster access to information [27, 36], improving well-being [16], or enhance occupational safety [4]. As these devices collect various data about their wearers, they pose potential risks to the wearer's privacy. Such risks may reduce the employees' acceptance. Therefore, it is recommended that companies record only work-related data and establish transparent processes to optimize the balance between advantages and associated risks [38]. Such transparency is also enforced in the GDPR, especially in Art. 5 (1) and Recitals 58 and 60. Although previous research on transparency mechanisms to increase privacy awareness exists [1, 3, 9, 17], none covers this aspect in the work-context, especially when considering data collection on smart watches. Thus, it is still unclear how transparency on smart watches should be implemented by employers in a work-context. Apart from this aspect, based on the GDPR, data subjects have also the right to control their data (e.g., GDPR, Art. 19). They have the right to revoke their consent to the processing at any time. This

allows control over the data as soon as it has been collected. However, the GDPR does not provide any reference to the possibility of temporarily interrupting data collection. While research on control mechanisms is done in private domains to control data collection [10, 19, 23, 37], none contributed insights about interrupting smart watch data collection when used in workplaces. As a result, we herein propose privacy-enhancing solutions tailored to employees using smart watches for working tasks. More precisely, we have designed three different transparency indicators showing when and which data collection occurs (see Fig. 5.4.1) and considered six different control interactions (see Fig. 5.5.1), which allow users to temporally interrupt the data collection. We have further explored the preferences of potential users for our proposed solutions using an online questionnaire. 1,033 participants contributed to our study. The key insights are as follows. Our participants prefer a splash-screen design to raise their awareness about actual data processing. The splash-screen design (see Fig. 5.4.1a) is like a notification on the smart watch screen, which requires the user's active involvement. Moreover, they want to be able to stop the data collection by preferably using a button in the menu of the work application running on the smart watch. Our results contribute to the privacy research regarding transparency and control in a work-context to enhance employees' privacy. Moreover, our findings could result in practical implications as employers can develop our findings in future smart watch applications used in smart workplaces to enhance employee transparency and control.

The remainder of the paper is structured as follows: In Sec. 5.2, we review related work. We present our research goals in Sec. 5.3. We detail our decision drivers in Sec. 5.4 and 5.5. We present our methodology in Sec. 5.6 and our results in Sec. 5.7, which we discuss in Sec. 5.8, and make concluding remarks in Sec. 5.9.

5.2 RELATED WORK

Related research can be classified into three categories: (1) privacy concerns, (2) raising privacy awareness, and (3) control mechanisms. The first category includes existing work on privacy concerns related to wearable devices. According to [31], privacy concerns are related to embedded sensors, which can measure, collect, and store data. Thereby, most concerns are indicated about revealing conversations, commuting, or stress [31]. Moreover, they found that users do not understand the implications of potential threats of collected data unless they have a personal connection to the data [31]. However, in the context of smart watches, privacy concerns can arise in many ways [13, 26], as individuals may have misconceptions or even false beliefs about these devices [39]. Regarding privacy concerns in the context of workplace environments, previous work highlights employees' concerns, including the fear of surveillance or tracking by the employer, or that the devices record sensitive information [7, 13, 33]. As a result, this can negatively impact workers' job satisfaction and stress levels, leading to productivity declines [22, 38].

In the second category, previous studies are dedicated to raising privacy awareness by nudging through visual indicators [17], warning messages [1, 3, 9, 34] or encouraging privacy-protective behavior [41]. However, the scope of these studies is limited to the private domain. The authors in [17] presented three approaches to raise user awareness when a front-face camera is accessed by an application. Their three approaches included designs using notification, frame, and camera preview and were evaluated by participants in a user study. The authors in [9] proposed a solution to increase users' privacy awareness

about threats in participatory sensing applications based on picture-based warnings. This empowers users to be informed about potential risks without having to read long texts. Other smartphone-based solutions are presented by [1, 3]. Both approaches provide detailed privacy information about the applications' behavior. However, they are designed for smartphones and not watches with different design constraints. Another work is the PATCOM project by [34]. They developed a smart watch application prototype, which can inform users when entering privacy-compromising environments. Hence, they provide some level of transparency by notifying users about the potential data collection, which can help strengthen trust in the environment. Finally, the approach in [41] raises privacy awareness with a game encouraging privacy-protective behavior for smart watch users but for private usages.

The third and last category deals with mechanisms to control data collection. Data control can be applied at different levels including stopping data collection, correcting and deleting data. Stopping sensors from collecting data usually leads to a disruption of the underlying service. Instead, users should be able to restrict sensor readings and still benefit from limited functions [8]. For example, smart speakers provide mute buttons to stop the microphone functions [19, 23]. However, the speakers can still be used for playing music. Another privacy-enhancing interaction is the privacy hat designed by [37], which has to be placed physically on top of the smart speaker to mute it. A more granular approach is proposed in [10] for smartphones with which users can separately control the collection of different sensor modalities.

To the best of our knowledge no previous work exists, which investigates employees' preferences regarding both (1) privacy indicators visualizing data collection on smart watches to increase employees' privacy awareness and (2) control interactions to interrupt data collection when equipped with a smart watch at work.

5.3 RESEARCH GOALS

Once employees themselves or the works council have consented to the collection of data through a collective agreement, employers can collect data about employees with the help of the smart watch according to the signed agreement. In this case, a one-time consent can generate a continuous data collection. Nevertheless, in accordance with the GDPR, employers must process personal data lawfully and transparently (GDPR, Art. 5 (1) a)), even though the GDPR leaves the regulations on the handling of employee data to the member states (GDPR, Art. 88). In general, the principle of Fair and Transparent Processing requires that the data subject is informed about the collection of personal data (GDPR, Recital 60). In detail, the principle of transparency requires that information about the processing should not only be easily accessible but also understandable (GDPR, Recital 39, 58). This can be supported by comprehensible visual elements, such as standardized symbols, which can provide an understandable overview of the processing (GDPR, Recital 60). To ensure that users are aware of the processing of personal data, we argue that privacy indicators can be used. Privacy indicators aim to provide individuals with meaningful information about how their privacy is being handled [32]. Such indicators may be textual, graphic, or audible [32]. Meanwhile, many IoT devices including smart speakers [11, 18, 19] are equipped with an LED that indicates data collection [30]. Motivated by the previously mentioned GDPR requirements and existing indicators, the question arises how employers can provide transparency about data collection for their

employees by using similar indicators tailored to smart watches. This leads to our first research question (RQ):

- RQ1: Which transparency indicator visualization(s) do employees perceive as sufficient and useful to be informed about the current data collection?

Transparency is often associated to the control over personal data by the data subjects themselves. Based on the GDPR, data subjects have the right to rectification (GDPR, Art. 16), erasure (GDPR, Art. 17), and restriction of processing (GDPR, Art. 19) of their data. In addition, a data subject has the right to object (GDPR, Art. 21). This allows the data subject to revoke their consent to the processing at any time. These rights allow control over the data as soon as it has been collected. Nevertheless, the GDPR does not provide any reference to the possibility of temporarily interrupting data collection. We argue that users should, however, be able to do so. This should also apply if a previously concluded company agreement allows the employers to collect data about their employees. The resulting self-determination of the employees to interrupt data collection can contribute in increasing their trust in the employers. However, such temporary interruptions in data collection can result in employers mistrusting employees using them. To prevent this scenario, additional mechanisms should be added to protect the employees. Nevertheless, in our scenario, the conditions of the interruptions are defined by the employers who provide the underlying application running on the smart watch. Therefore, we aim at addressing the following research question:

- RQ2: Which interaction(s) is/are perceived by the employees as appropriate to control the data collection?

5.4 PRIVACY INDICATORS

Our first objective is to indicate data collection with privacy indicators to provide transparency about it. In what follows, we motivate our design decisions based on an analysis of existing drivers and detail our resulting designs.

5.4.1 *Design Drivers*

To design our privacy indicator, we consider two factors: (1) notification of the data collection and (2) the display of the related information that affect the design of the subsequent layout on smart watches. Firstly, notifications are visual, auditory, or haptic stimuli triggered by applications or services to relay information that are outside of the scope of users' attention. Auditory or haptic stimuli are especially efficient in interrupting users activities to gain their attention [5]. These interruptions can be perceived as intrusive and annoying, especially when the wearer receives numerous notifications [25, 28, 40]. For example, results in [40] indicate that notifications of a messenger application were perceived as less annoying than the notifications of a music application because these notifications were of lesser interest. Therefore, the notifications should be of interest, i.e., perceived as useful to the user. Moreover, they should be used with care to avoid habituation effects.

Secondly, smart watches are constrained by size and shape. Compared to smartphones, their screen is even smaller. Since smart watch wearers only briefly check the screen [29],

the provided information should be as brief as possible to accommodate the screen size and not to appear cluttered, while providing concise and understandable information about ongoing data collection. Moreover, it should cater to existing smart watch forms including round or square screens.

Thirdly, in the context of smart workplaces, the collection of activity, health, and location data are possible. An indication of such data collection needs to be easy to understand and fast to distinguish. Therefore, the presentation of the ongoing data collection of the different data types should differ at least in color. A double coding should be introduced to cater for color-blind users.

5.4.2 *Resulting Designs*

We present our privacy indicators which were created based on the aforementioned design drivers. Hereby, the currently available smart watch operating systems serve as basis for our design decisions.

(a) Splash-screen design (b) Circular design (c) Icon design

Figure 5.4.1: Examples of proposed indicators to visualize the collection of health data on a smart watch

DESIGN A: SPLASH-SCREEN The first design shown in Fig. 5.4.1a is the most common and known as a notification. It is motivated by [17, 34] and represents a normal notification, which the wearer must actively close. The used color depends on the collected data type(s). We have attributed blue to activity data, red to health data, and yellow to location data. In addition to color, the splash-screen design offers an icon and an additional text to further inform the wearers. In addition, it can be supported by an auditory or haptic signal. Possible limitation of this indicator are that (1) it prevent users from seeing anything else on the screen and (2) requires an explicit interaction to close it. As a result, the wearers' attention may be improved but at the cost of more efforts.

DESIGN B: CIRCLE The second design shown in Fig. 5.4.1b and motivated by [17] is a circle that surrounds the watch face and differs in color based on the data type following the same color scheme as above. In addition, a supportive icon is added. The circle indicator is displayed for a few seconds and can also be supported by an auditory or haptic signal. During data collection, the circle appears around the watch face and disappears when the data collection stops. This means that the wearers are constantly informed about the current data collection. If neither an auditory signal nor vibration is added, this indicator is a very reduced and simple way to notify the wearer about data collection when the wearer is looking at the watch face. Its advantage is that it uses the

watch face and does not cover it or require any action from the wearer as compared to the previous design. However, its simplicity may negatively affect the wearer's understanding at the beginning, as the color is only mapped with an icon and no additional information.

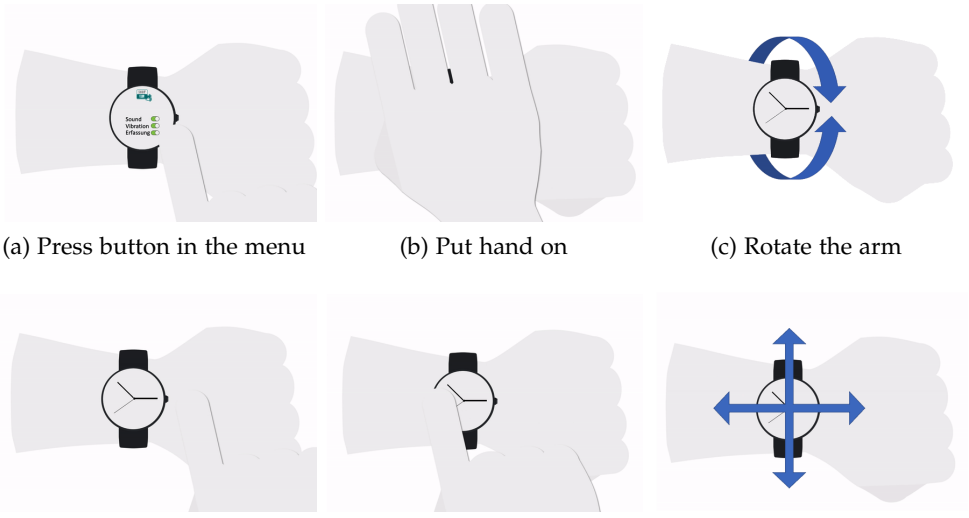
DESIGN C: ICON Our last design shown in Fig. 5.4.1c and motivated by [2] is a bigger visual cue on the watch face at the top of the smart watch screen. It consists of a bigger colored icon. Auditory or haptic stimuli can also extend the design. As with the previous design, the respective indicator is visible for a few seconds. As soon as data collection is active, the indicator on the watch face appears. As compared to design B, the circle with the small icon is replaced by a bigger icon on the watch face. A bigger size could mitigate the mentioned weakness of design B. However, the indicator is only visible when the wearer actively looks at the smart watch in contrast to design A.

5.5 CONTROL INTERACTIONS

Our second objective is to allow users to control the data collection by temporarily interrupting it. This objective aims to support employees in controlling their personal information and refers to the right to restrict personal information processing (GDPR, Art. 18).

5.5.1 *Design Drivers*

To allow such control, the corresponding interactions should be easy to understand and executable by the wearers in different situations. The chosen interactions should also take into about the wearers' physical capabilities and be reliably recognized by the smart watch. The possible interaction options are via touchscreen, buttons, frame, and sensors that detect arm movement.



(a) Press button in the menu (b) Put hand on (c) Rotate the arm

(d) Press a button on the side 2 times (e) Perform a movement on the frame (f) Perform a gesture

Figure 5.5.1: Proposed mechanisms to interrupt personal data collection on a smart watch

5.5.2 *Selected Control Interactions*

In the following, we describe the selected control interactions illustrated in Fig. 5.5.1, which enable the user to interrupt the data collection.

INTERACTION A: PRESS A BUTTON IN THE MENU Fig. 5.5.1a represents a manual interaction, as the wearer needs to open the respective application, go through the settings and deactivate the data collection using a button. This is advantageous as users are usually familiar with the use of menus. However, the interaction requires different steps.

INTERACTION B: PUT HAND ON Fig. 5.5.1b presents an interaction leveraging the ambient light sensor of the smart watch. Every time the wearer covers this sensor with the palm, the data collection stops. For this interaction, no further steps are needed. This interaction is easy to perform, but could foster many false interruptions depending on the deployment scenarios.

INTERACTION C: ROTATE THE ARM Fig. 5.5.1c shows an interaction based on a hand gesture by rotating the arm with the smart watch in a specific manner. As soon as the smart watch sensors detect the movement, the data collection is interrupted. Although this interaction only requires an easy arm rotation, it causes the screen to be out of the wearers' view. Furthermore, this interaction can be triggered unintentionally.

INTERACTION D: PRESS A BUTTON ON THE SIDE Fig. 5.5.1d shows the easiest to understand interaction after the menu interaction. The smart watch wearer presses the mechanical button at the side of the watch to stop the collection. This interaction is easy to perform and easy to remember. To avoid false positive interruptions, the button needs to be pressed two times.

INTERACTION E: PERFORM A MOVEMENT ON THE FRAME Fig. 5.5.1e presents a finger gesture performed on the smart watch frame. The wearer has to touch the frame and swipe down, for example. This interaction is easy to remember as it needs to be performed at the smart watch's frame. However, wearing gloves can hinder performing it as the device could not recognize the finger, for instance.

INTERACTION F: PERFORM A GESTURE Fig. 5.5.1f shows our second real gesture. Similar to the gesture in Fig. 5.5.1c, the wearer has to perform a hand movement. Here, the hand movement is a movement in the air using a special pattern.

In summary, we consider three designs for the privacy indicators and six different interactions to control the data collection in what follows.

5.6 METHODOLOGY

5.6.1 *Survey Distribution*

To answer our research questions, we have conducted an online questionnaire conforming to the GDPR and approved by the Data Protection Officer of our university. While we

do not have a formal IRB process at our university, we have taken particular care to minimize potential harms to the participants, by, e.g., reducing the number of questions to the minimum to avoid fatigue. Participants have been informed that they could leave the questionnaire at any time. The questionnaire has been distributed by a panel certified ISO 26362 and the participants have been financially rewarded. Our inclusion criteria were that our participants had to be between 18 and 67 years old, living and working full-time in Germany. Participants were chosen based on quotas, i.e., the distribution in terms of age and gender is representative of the German population [35]. In total, 1,033 participants answered our questionnaire in August 2021.

5.6.2 *Survey Design*

Our questionnaire is articulated around a smart workplace scenario, in which the participants have to imagine that they are equipped with smart watches when performing their jobs. After starting with demographics questions to fulfill the survey quotas, the main questionnaire starts. In the first part, we analyze their preferences for three different smart watch indicators introduced in Sec. 5.4.2 displayed on the smart watch when data is collected. For each indicator we propose an alternative in color and related icon for different collected data types: Activity, health, and location. For example, Fig. 5.4.1 shows the three different alternatives for health data. Based on these alternatives, we ask the participants different questions to elicit their preferences on a 5-point Likert scale from "strongly disagree" to "strongly agree". Then, in the second part, we investigate the scenarios in which they would like to control the data collection and propose different interactions for each data type (see Fig. 5.5.1). Each interaction is illustrated by an animation, so that our participants could understand the interactions more easily. Later in the questionnaire, we ask our participants questions regarding their smart watch ownership, usage, and main purpose. To elaborate on our participants' technical affinity, we ask nine questions with a 6-point Likert scale from "completely disagree" to "completely agree" proposed by [14]. At the end of the questionnaire, we finally ask our participants to provide work-related information, including the sector, work function, work environment, and work conditions based on predefined choices. The questionnaire is available online (`https://owncloud.gwdg.de/index.php/s/YGW2QXRHsJ5y8Nv`).

5.7 RESULTS

5.7.1 *Demographics*

Among our 1,033 participants, 48% are women and 52% are men. Their age distribution matches the current population of Germany [35]. A majority of our participants work in health and social care (15%) followed by industry (14%), public service (7%), and IT/telecom (6%). Their working conditions are as follows: 90% work inside, 64% in quiet environments, and 63% walk rather little during work. Interestingly, 43% already own a smart watch. Overall, more females (47%) than males (40%) stated that they own a smart watch. A Mann-Whitney U test indicates that gender is a significant influence ($p = .013$). Likewise, age ($p < .001$, Kruskal-Wallis test). Especially younger participants own a smart watch. A pairwise comparison (Bonferoni-Correction) reveals significant differences between the age categories 18-24 and 45-54 ($p < .001$), 18-24 and 55-67 ($p < .001$), 25-34

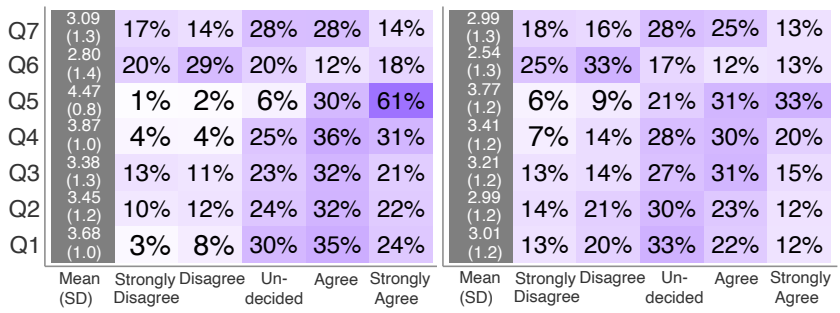
and 45-54, ($p < .01$), 25-34 and 55-67 ($p = .01$), 35-44 and 45-54, ($p < .01$), as well as 35-44 and 55-67 ($p = .01$). The majority (70%) use their smart watch daily. Although about 79% use their smart watch mainly for private purposes (79%), some indicated that they use it also for work (19%) or even exclusively for work (2%). Regarding the results based on the technical affinity score proposed by [14], we assume that our participants are rather tech-savvy. Overall, all participants reach a mean score of 3.94 ($SD = 0.96$) on a scale from one to six. A closer look reveals that males ($M = 4.18, SD = 0.92$) reach significantly ($p = .05$) higher scores than females ($M = 3.68, SD = 0.93$). While gender has an impact, age does not.

5.7.2 *Preferences for Privacy Indicators*

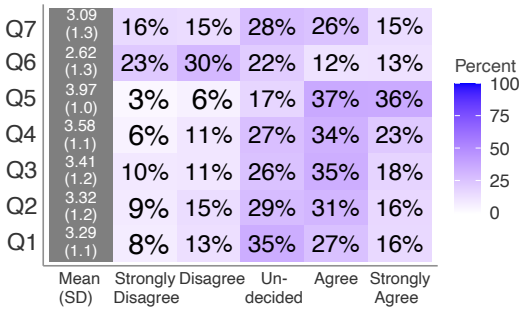
When considering our three privacy indicators (see Fig. 5.4.1), the results indicate that our participants prefer the splash-screen design (38%) followed by the icon design (34%) and the circle design (28%). A closer look at our results regarding the seven sub-questions (see. Fig. 5.7.1) about how the data collection is presented shows a similar picture. The seven questions reach a Cronbach's Alpha of 0.86, indicating acceptable reliability [12]. In all sub-questions, except sub-question three, the splash-screen design reaches higher means, shown in Fig. 5.7.1. Our participants think that the splash-screen design would better raise their general awareness about privacy issues ($M = 3.45, SD = 1.2$) and increase their awareness about the data collection ($M = 3.68, SD = 1.0$) than the other two indicators in both cases. However, they are rated similarly in terms of acceptance. Although the notification presented in the splash-screen design is not new, our participants find it on average more intuitive ($M = 3.87, SD = 1.0$) than the circle ($M = 3.41, SD = 1.2$) or icon ($M = 3.58, SD = 1.1$) design. In general, the results indicate that the splash-screen design, on average, is the easiest to understand for our participants. However, this indicator is estimated to be the most disturbing in comparison to the other two.

5.7.3 *Additional Feedback.*

Regarding additional signals such as vibration or sound, the results show that 48% of our participants would like to have auditory feedback. A qualitative content analysis [21] shows that the open answers from proponents of auditory feedback most frequently relate to *awareness, informed, or remembered*, while those from opponents frequently relate to the categories *disturbing, annoying, or distracting* instead. In contrast, 58% would wish for a complementary haptic feedback. The most frequent categories based on the proponents' answers are *less disturbing, awareness, remembered, informed, more discrete*, while the opponents' answer categories are similar to those from the auditory opponents. While a χ^2-test reveals, that only gender ($\chi^2_{(1)} = 7.34, p = .007$) has a significant relationship with participants' decision on additional sound, gender ($\chi^2_{(1)} = 4.29, p < .04$), age ($\chi^2_{(4)} = 20.15, p < .001$), and smartwatch ownership ($\chi^2_{(1)} = 37.26, p < .001$) significantly relate to additional vibrations.



(a) Splash-screen (b) Circle



(c) Icon

Figure 5.7.1: Results of proposed privacy indicators. Attitude on "This privacy indicator... (Q1) would reinforce my perception about data collection. (Q2) would catch my general attention. (Q3) seems to me to be useful for the purpose. (Q4) is intuitive. (Q5) is easy to understand. (Q6) is disturbing. (Q7) is acceptable in order to visualize the data collection."

5.7.4 *Deactivation Option.*

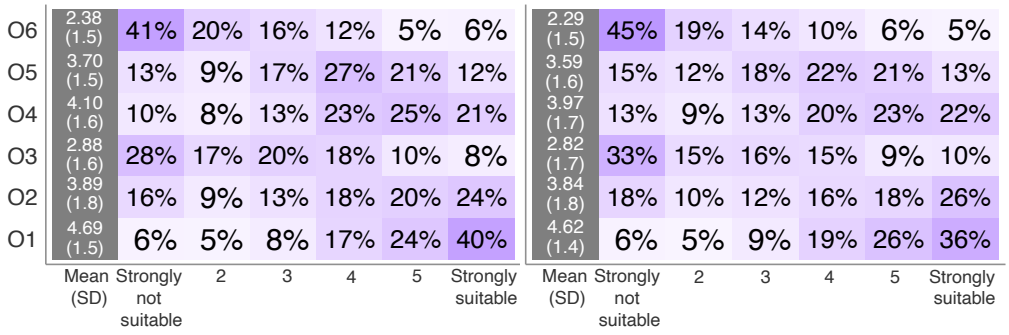
When it comes to the question to deactivate such an indicator, their answers reveal that 32% would rather deactivate such privacy indicators. Statements include *"I don't think it's essential to know when it's being recorded"* (participant 289) or *"may be disruptive in meetings"* (participant 69). A χ^2-test reveals, a significant relationship with gender ($\chi^2_{(1)} = 5.64, p = .02$), age ($\chi^2_{(4)} = 18.22, p = .001$), and ownership ($\chi^2_{(1)} = 15.67, p < .001$).

5.7.5 *Preferences for Control Interactions*

Concerning the interruption of data collection, 67% of our participants "strongly agree" (48%) or "agree" (19%) that they would like to have this opportunity. Overall, our participants indicated they would like to interrupt data collection in private scenarios for all data types (i.e., activity, health, location) and during the walk to the toilet (67%), or when having breaks (65%) when, e.g., the location would be collected. The detailed results are shown in Tab. 5.7.1 and suggest similar results among the different data types. When considering the different proposed mechanisms to interrupt data collection, a majority (51%) would prefer to press a button in the menu. In comparison, arm movements like arm rotation or another arm gesture are less desired. Fig. 5.7.2 show the results for each

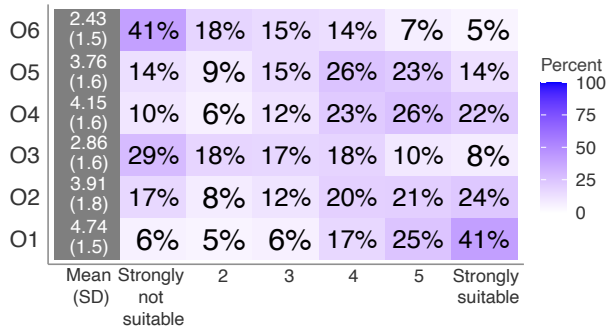
Table 5.7.1: Employees' selection of situations to interrupt data collection

Case	Activity	Health	Location	Private Context
During concentration periods	21%	21%	21%	
During a private conversation	40%	42%	42%	✓
During professional meeting	23%	26%	23%	
While smoking	24%	23%	29%	✓
While eating	52%	56%	52%	✓
During the break	61%	62%	65%	✓
During the walk to the toilet	61%	65%	67%	✓



(a) Activity

(b) Health



(c) Location

Figure 5.7.2: Results of employees' attitude on the suitability of smart watch interactions: (O1) Press a button in the menu, (O2) Put your hand on, (O3) Rotate the arm, (O4) Press a button on the side 2 times, (O5) Perform a movement on the frame, (O6) Perform a gesture

interaction option on the scale from "strongly not suitable" to "strongly suitable" for all data types. Along all data types, our participants do not differ much between the presented interactions.

5.8 DISCUSSION

We next discuss the results obtained for the privacy indicators followed by those for the control interactions. We finally address the limitations of this work.

5.8.1 *Privacy Indicators*

Our first research question (see Sec. 5.3) focuses on analyzing which privacy indicators are perceived by employees as sufficient and useful to visualize data collection. The results described in Sec. 5.7 reveal that our participants prefer the splash-screen design. This is surprising as this design requires an additional and active action from the users to be able to access the main screen of the watch. In contrast, both other designs do not require a dedicated interaction from the users. One of the reasons to explain this result might be that our participants are already familiar with notifications from other applications or smart devices based on a similar interaction. However, the differences in terms of preferences between the splash-screen design and the other designs remain low. The icon design is the next preferred design following the splash-screen design. In particular, when asked whether the representations appear useful for the intended purpose, the results show that all participants gave a similar rating for all proposed indicators. Since the performance of the three proposed designs remains similar, we suggest that employers could let employees choose from different indicators according to their preferences.

5.8.2 *Additional Feedback.*

In addition to the visual elements of such indicators, the results shown in Sec. 5.7 indicate that participants' opinions differ regarding supplementary feedback, either a sound or vibrations. Thus, the findings from [24] differ from ours as the existing results indicate that those participants prefer soundless privacy nudges, as they are not annoying, intrusive, or interruptive in a private context. Besides, prior research found that users have to deal with tons of notifications daily [28] and that such notifications are disruptive on smartphones [25, 28]. A reduction of those interruptions could be possible in a professional context by deferring notification [28], especially when it comes to privacy notifications, as users usually consider standard app notifications to be more important than privacy notifications [24]. Therefore, less noticeable notifications such as silent mode should be possible [24] because even then, privacy notifications would be read according to [24]. Employers should therefore consider this aspect when informing their employees about current data collection. Again, existing work extended by our gained insights suggest that employers should support individuals' preferences and offer different options regarding privacy indicators. We however recommend that they should also consider the working environments of their employees to take into account potential safety issues that might arise if employees would be distracted by a acoustic or haptic notification during their tasks.

5.8.3 *Deactivation Option.*

Our results indicate that one-third of our participants would like to disable these indicators. However, most would not. This highlights that employees would like to know when data collection arises. However, we recommend employers to let the last decision from the employees' perspective so that they can disable it when they want to, as it was not intended to be distracting.

5.8.4 *Control Interactions*

Overall, our results presented in Sec. 5.7, indicate that our participants want to have the control to interrupt employers' data collection when working with a smart watch. This possibility is especially wished for in situations considered as private by our participants. Such situations include private conversations, breaks, or going to the toilet. From the obtained results, employers should hence provide such an option. The realization of this function can be done by different control interactions. Considering our second research question (see Sec. 5.3), our results indicate that our participants prefer to (1) press a button in the menu or (2) interact with a physical button on the smart watch to stop the data collection. As a result, they potentially chose an interaction that may be more familiar to them. Other interactions may not have been imaginable in their working environments. For example, raising an arm and making arm gestures seems inappropriate when sitting in an office in front of a colleague, while it could be imaginable in an industrial scenario. Hence, this confirms that employees would like to have more discrete interactions. Note that the participants' preferences only slightly differ for the different considered data types (i.e., health, location, and activity).

5.8.5 *Limitations*

Since the conducted study is based on an online questionnaire, the answers provided by our participants reflect their claimed opinions and not necessarily their actual behavior. Moreover, we have submitted them a scenario that they should imagine. As a result, what they imagined may differ between participants. This is beneficial as the participants may have adapted their thoughts to their own working context, which is not possible to do with our questionnaire. However, we cannot be sure that this is the case. As a result, the exploration conducted in this study should be confirmed by future real-world experiments in context.

Some of our participants did not own a smart watch yet. As a result, they needed to imagine how it would be and their answers are likely influenced by previous experiences with other devices. However, we have decided to also ask them about their preferences, as we have assumed that they could be more reluctant about data collection than actual users. Such differences could however not be observed. We have finally focused in our study on German employees over 18. Our results may hence differ with younger working participants or other cultures. This cross-cultural aspect will be considered in future work when conducting our next study in context. Our results may finally not be applicable in other application areas due to the known dependency of privacy-related decisions on context.

5.9 CONCLUSIONS

We have investigated employees' preferences for different proposed privacy indicators to raise awareness about data collection and control interactions to stop this collection. To this end, we have conducted an online questionnaire-based study with 1,033 full-time employed participants to get first insights about their preferences. Our results indicate that our participants prefer the splash-screen indicator (Fig. 5.4.1a) to visualize data collection followed by the icon (Fig. 5.4.1c) and the circle indicator (Fig. 5.4.1b). The participants are, however, split about their preferences to have an additional haptic or auditory feedback. Being able to interrupt data collection is important for our participants, especially in more private situations. Their willingness to do so does not significantly vary with the collected data types. Similarly to the privacy indicators, our participants tend to prefer the interaction they are familiar with. The majority prefers doing it via a menu interaction with virtual buttons. While our results provide a first exploration of employees' preferences, more efforts including real-wold studies in context are needed to be able to provide usable transparency and control to employees in smart workplaces. Such provision could be beneficial for both employees and employers. The former would benefit from more transparency and control that could increase their trust in the latter, thus fostering their acceptance of smart workplaces.

ACKNOWLEDGMENTS.

We would like thank our participants and our group members for their feedback on the questionnaire.

REFERENCES

[1] H. Almuhimedi, F. Schaub, N. Sadeh, I. Adjerid, A. Acquisti, J. Gluck, L. F. Cranor, and Y. Agarwal. "Your Location Has Been Shared 5,398 Times! A Field Study on Mobile App Privacy Nudging." In: *Proc. of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. 2015.

[2] Apple Inc. *About the orange and green indicators in your iPhone status bar*. 2017. URL: https://support.apple.com/en-us/HT211876 (visited on 09/09/2021).

[3] G. Bal, K. Rannenberg, and J. Hong. "Styx: Design and Evaluation of a New Privacy Risk Communication Method for Smartphones." In: *Proc. of the 29th IFIP International Information Security, Conference (SEC)*. 2014.

[4] J. Barata and P. R. da Cunha. "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)*. 2019.

[5] P. P. Bovard, K. A. Sprehn, M. G. Cunha, J. Chun, S. Kim, J. L. Schwartz, S. K. Garver, and A. K. Dey. "Multi-Modal Interruptions on Primary Task Performance." In: *Proc. of the 12th International Conference on Augmented Cognition (AC)*. 2018.

[6] CCS Insight. *Healthy Outlook for Wearables As Users Focus on Fitness and Well-Being*. 2021. URL: https://www.ccsinsight.com/press/company-news/healthy-outlook-for-wearables-as-users-focus-on-fitness-and-well-being/ (visited on 05/21/2021).

[7] B. Choi, S. Hwang, and S. H. Lee. "What Drives Construction Workers' Acceptance of Wearable Technologies in the Workplace?: Indoor Localization and Wearable Health Devices for Occupational Safety and Health." In: *Automation in Construction* 84.1 (2017).

[8] D. Christin, F. Engelmann, and M. Hollick. "Usable Privacy for Mobile Sensing Applications." In: *Proc. of the 8th Workshop on Information Security Theory and Practice (WISTP)*. Vol. 8501. 2014.

[9] D. Christin, M. Michalak, and M. Hollick. "Raising User Awareness about Privacy Threats in Participatory Sensing Applications through Graphical Warnings." In: *Proc. of the 11th International Conference on Advances in Mobile Computing & Multimedia (MoMM)*. 2013.

[10] D. Christin, A. Reinhardt, M. Hollick, and K. Trumpold. "Exploring User Preferences for Privacy Interfaces in Mobile Sensing Applications." In: *Proc. of 11th ACM International Conference on Mobile and Ubiquitous Multimedia (MUM)*. 2012.

[11] H. Chung, M. Iorga, J. M. Voas, and S. Lee. "'"Alexa, Can I Trust You?"." In: *Computer* 50.9 (2017).

[12] J. M. Cortina. "What Is Coefficient Alpha? An Examination of Theory and Applications." In: *Journal of applied psychology* 78.1 (1993).

[13] P. Datta, A. S. Namin, and M. Chatterjee. "A Survey of Privacy Concerns in Wearable Devices." In: *Proc. of the IEEE International Conference on Big Data (Big Data)*. 2018.

[14] T. Franke, C. Attig, and D. Wessel. "A Personal Resource for Technology Interaction: Development and Validation of the Affinity for Technology Interaction (Ati) Scale." In: *International Journal of Human–Computer Interaction* 35.6 (2019).

[15] Gartner Inc. *Gartner Forecasts Global Spending on Wearable Devices to Total $81.5 Billion in 2021*. 2021. URL: https://www.gartner.com/en/newsroom/press-releases/2021-01-11-gartner-forecasts-global-spending-on-wearable-devices-to-total-81-5-billion-in-2021 (visited on 02/14/2021).

[16] D. G. Glance, E. Ooi, Y. Berman, C. F. Glance, and H. R. Barrett. "Impact of a Digital Activity Tracker-Based Workplace Activity Program on Health and Wellbeing." In: *Proc. of the 6th International Conference on Digital Health Conference (DH)*. 2016.

[17] M. Hassib, H. Abdelmoteleb, and M. Khamis. "Are my Apps Peeking? Comparing Nudging Mechanisms to Raise Awareness of Access to Mobile Front-facing Camera." In: *Proc. of the 19th International Conference on Mobile and Ubiquitous Multimedia (MUM)*. 2020.

[18] L. Hernández Acosta and D. Reinhardt. "A Survey on Privacy Issues and Solutions for Voice-Controlled Digital Assistants." In: *Pervasive and Mobile Computing* (2021).

[19] J. Lau, B. Zimmerman, and F. Schaub. "Alexa, Are You Listening?: Privacy Perceptions, Concerns and Privacy-seeking Behaviors with Smart Speakers." In: *ACM Human-Computer Interactions* 2.CSCW (2018).

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

[21] P. Mayring. "Qualitative Content Analysis." In: *A companion to qualitative research* 1.2 (2004).

[22] N. Meyers. "Employee Privacy in the Electronic Workplace: Current Issues for IT Professionals." In: *Proc. of the 14th Australasian Conference on Information Systems (ACIS)*. 2003.

[23] A. H. Mhaidli, M. K. Venkatesh, Y. Zou, and F. Schaub. "Listen Only When Spoken To: Interpersonal Communication Cues as Smart Speaker Privacy Controls." In: *Proc. of the 20st Privacy Enhancing Technologies Symposium (PoPETs)*. 2020.

[24] N. Micallef, M. Just, L. Baillie, and M. Alharby. "Stop Annoying Me! An Empirical Investigation of the Usability of App Privacy Notifications." In: *Proc. of the 29th Australian Conference on Computer-Human Interaction (OZCHI)*. 2017.

[25] S. Mirzamohammadi and A. A. Sani. "Viola: Trustworthy Sensor Notifications for Enhanced Privacy on Mobile Systems." In: *IEEE Transactions on Mobile Computing* 17.11 (2018).

[26] V. G. Motti and K. Caine. "Users' Privacy Concerns About Wearables." In: *International Conference on Financial Cryptography and Data Security*.

[27] M. Peissner and C. Hipp. *Potenziale der Mensch-Technik-Interaktion für die effiziente und vernetzte Produktion von morgen*. Fraunhofer-Verlag Stuttgart, 2013.

[28] M. Pielot, K. Church, and R. de Oliveira. "An In-Situ Study of Mobile Phone Notifications." In: *Proc. of the 16th International Conference on Human-Computer Interaction with Mobile Devices amp; Services (MobileHCI)*. 2014.

[29] S. Pizza, B. Brown, D. McMillan, and A. Lampinen. "Smartwatch in Vivo." In: *Proc. of the 34th Conference on Human Factors in Computing Systems (CHI)*. 2016.

[30] S. Prange, A. Shams, R. Piening, Y. Abdelrahman, and F. Alt. "PriView- Exploring Visualisations to Support Users' Privacy Awareness." In: *Proc. of the ACM Conference on Human Factors in Computing Systems (CHI)*. 2021.

[31] A. Raij, A. Ghosh, S. Kumar, and M. Srivastava. "Privacy Risks Emerging from the Adoption of Innocuous Wearable Sensors in the Mobile Environment." In: *Proc. of the 29th ACM Conference on Human Factors in Computing Systems (SIGCHI)*. 2011.

[32] J. R. Reidenberg, N. C. Russell, V. Herta, W. Sierra-Rocafort, and T. B. Norton. "Trustworthy Privacy Indicators: Grades, Labels, Certifications, and Dashboards." In: *Wash. UL Rev.* 96 (2018).

[33] M. C. J. Schall, R. F. Sesek, and L. A. Cavuoto. "Barriers to the Adoption of Wearable Sensors in the Workplace: A Survey of Occupational Safety and Health Professionals." In: *Human Factors* 60.3 (2018).

[34] P. A. Shaw, M. A. Mikusz, N. A. J. Davies, and S. E. Clinch. "Using Smartwatches for Privacy Awareness in Pervasive Environments." In: *Poster at the 18th International Workshop on Mobile Computing Systems and Applications (HotMobile)* (2017).

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

[36] A. Stocker, P. Brandl, R. Michalczuk, and M. Rosenberger. "Mensch-zentrierte IKT-Lösungen in einer Smart Factory." In: *e & i Elektrotechnik und Informationstechnik* 131.7 (2014).

[37] C. Tiefenau, M. Häring, E. Gerlitz, and E. von Zezschwitz. "Making Privacy Graspable: Can we Nudge Users to use Privacy Enhancing Techniques?" In: *CoRR* (2019).

[38] D. L. Tomczak, L. A. Lanzo, and H. Aguinis. "Evidence-based Recommendations for Employee Performance Monitoring." In: *Business Horizons* 61.2 (2018).

[39] E. S. Udoh and A. Alkharashi. "Privacy Risk Awareness and the Behavior of Smartwatch Users: A Case Study of Indiana University Students." In: *Proc. of the 2016 Future Technologies Conference (FTC)*. 2016.

[40] D. Weber, A. Voit, H. V. Le, and N. Henze. "Notification Dashboard: Enabling Reflection on Mobile Notifications." In: *Proc. of the 18th International Conference on Human-Computer Interaction with Mobile Devices and Services Adjunct (MobileHCI)*. ACM, 2016.

[41] M. Williams, J. R. Nurse, and S. Creese. "(Smart) Watch Out! Encouraging Privacy-Protective Behavior Through Interactive Games." In: *International Journal of Human-Computer Studies* 132 (2019).

[42] Zebra Technologies. *Quality Drives a Smarter Plant Floor: Manufacturing Vision Study*. 2017. URL: `https://www.zebra.com/content/dam/zebra_new_ia/en-us/solutions-verticals/vertical-solutions/manufacturing/white-papers/2017-manufacturing-vision-study-en-emea.pdf` (visited on 09/21/2021).

PAPER V

6

PRIVACY-PRESERVING HUMAN-MACHINE CO-EXISTENCE ON SMART FACTORY SHOP FLOORS

ABSTRACT. Smart factories are characterized by the presence of both human actors and AGVs for the transport of materials. To avoid collisions between workers and AGVs, the latter must be aware of the workers' location on the shop floor. Wearable devices like smart watches are a viable solution to determine and wirelessly transmit workers' current location. However, when these locations are sent at regular intervals, workers' locations and trajectories can be tracked, thus potentially reducing the acceptance of these devices by workers and staff councils. Deliberately obfuscating location information (*spatial cloaking*) is a widely applied solution to minimize the resulting location privacy implications. However, a number of configuration parameters need to be determined for the safe, yet privacy-preserving, operation of spatial cloaking. We comprehensively analyze the parameter space and derive suitable settings to make smart factories safe and cater to an adequate privacy protection workers.

KEYWORDS. Smart Factory · Spatial Cloaking · Privacy Protection.

CITATION. A. Richter, A. Reinhardt, and D. Reinhardt. Privacy-Preserving Human-Machine Co-Existence on Smart Factory Shop Floors. Proceedings of the 2nd International Workshop on Simulation Science. SimScience 2019. 2020.

6.1 INTRODUCTION

The digital revolution has reached industry shop floors around the globe. Besides leading to an optimization of manufacturing processes, it also fundamentally changes the way the employees work. Companies are increasingly relying on the support of industrial robots for assisting in manufacturing processes and goods transport. Autonomous robots have particularly emerged as viable solutions for material transport between storage areas and workplaces. These autonomous robots, also referred to as AGVs, facilitate the autonomous supply of workplaces with materials from warehouses, without the need for human interaction. Sales forecasts for AGVs show an increasing trend for companies to use more AGVs for transport processes in the future [20]. This inevitably leads to an increasing co-existence between humans and robots on the shop floors of smart factories.

The digitalization of manufacturing processes is also changing the way workers work on shop floors. Companies optimize their processes by increasingly promoting the use of wearable computing devices [23] to increase workers' productivity [21, 24, 27], health [11, 12, 18], and safety [6]. Wearable devices like smart watches, smart vests, or smart glasses [1, 30] already support workers by instructing them or providing them with additional process-related information [21, 24]. Moreover, they can contribute to workers' health and safety through their built-in sensors because their data allow for the

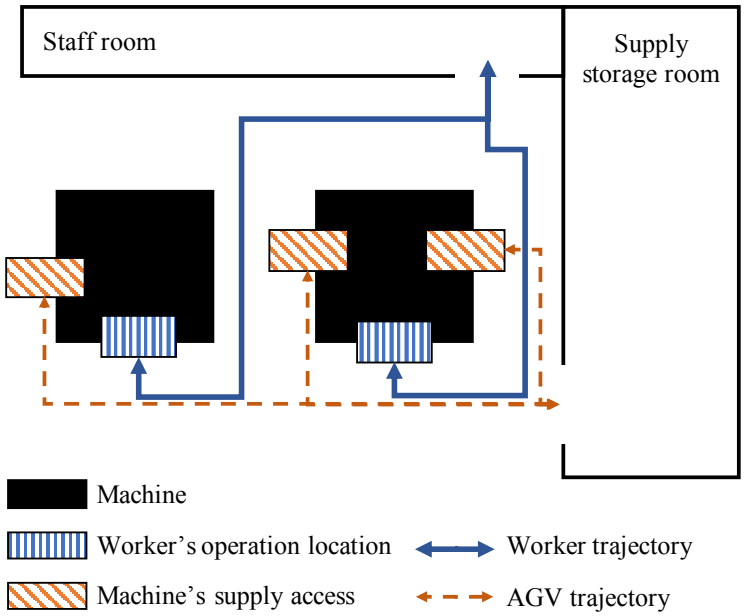


Figure 6.2.1: Sample layout of a shop floor in a smart factory.

recognition of user activities, such as walking, standing, sitting, and even the workers' position on the shop floor [2, 17].

Connected wearable devices, worn by workers, can inform AGVs about their current locations. This knowledge of the workers' locations prevents AGVs from colliding with humans. There is, however, a downside to a frequent reporting of location information, namely the ensuing threats to the workers' location privacy. Such threats can lead to a reduced acceptance of smart wearables by workers. We therefore investigate the applicability of a location privacy protection techniques in a smart factory scenario. More precisely, we present an extensive simulation study to assess existing trade-offs between AGVs' routing and workers' privacy protection. The rest of the paper is structured as follows. In Section 6.2, we briefly revisit our definition of smart factories and elaborate on the co-existence of workers and AGVs on the shop floors in industrial environments. Section 6.3 discusses the resulting privacy implications and existing location privacy preserving techniques. We introduce simulation parameters, objectives, and methodology of our study in Section 6.4, before discussing the corresponding results in Section 6.5. At last, Section 6.6 concludes this paper.

6.2 THE SMART FACTORY

Smart factories are characterized by the presence of AGVs and other robots that contribute to industrial processes [13]. For the AGVs' coordination, a large volume of information is collected and exchanged between participating devices. This enables seamless, safe, and secure interactions between humans, machines, material, and systems [19, 22, 29]. Human workers still take an important role in smart factories, because of their in-depth understanding of dependencies between process steps and their capability to adequately react to unexpected situations. We thus anticipate that human-machine interactions will continue to exist on shop floors for many years to come.

In this scenario, problems can occur due to the limited space available on the shop floor, though. Often, workers and AGVs need to share the available space (see Fig. 6.2.1 for an example). On smart factory shop floors, AGVs are expected to transport materials between machines and workplaces. Their autonomy allows them to collect and deliver items when and where they are needed. Since AGVs move independently between different places, it is of particular importance that AGVs know the positions of the human workers sharing the shop floor, in order to reduce their speed or even completely stop in the case of an impending collision. Diverse options exist to proactively prevent collisions between AGVs and workers. Most often, this collision prevention is realized through equipping the autonomous robots with detectors for the human presence, and stopping their operation while a human is present in their immediate environment. Diverse technologies can support human detection. On the one hand, AGVs can be equipped with infrared sensors to detect body heat, radar sensors or laser rangefinders to recognize the shape of human bodies, or cameras to locate humans and anticipate their movements [15]. Particularly, laser rangefinders are often used to detect obstacles on shop floors [10]. However, in that case, the AGVs would not be able to optimize their trajectories in advance. On the other hand, workers can be equipped with wearable devices that periodically broadcast their current position on the shop floor, and thus allow nearby AGVs to stop if they come too close. A strong advantage of the latter type of solutions is their capability to detect workers even when they are not within the camera's field of view. Additionally, such wearable devices can also bring benefits for the workers, such as displaying additional information to accelerate the execution of their tasks [21, 24]. The increasing number of smart wearables in companies [23] suggests that companies may want to benefit from the advantages offered by these products in the future. Thus, we follow the latter option, and assume that smart wearables (e.g., smart watches) are worn by the workers in this paper. We further assume that the smart wearables know the workers' location information and can broadcast it wirelessly in order to make it known to the AGVs.

6.3 PRIVACY IMPLICATIONS OF WEARABLES IN SMART FACTORIES

The regular transmission of location information has strong implications on user privacy. Transmitted information enables the employer to closely monitor workers' routines (e.g., their breaks or work efficiency), categorize them, and eventually even draw inferences about a worker's performance. Even if no unique user identifiers are transmitted, the AGVs receiving the workers' positions and movements can be tracked based on the constant stream of location information. If the AGVs collude with each other by exchanging their own positions and the times when encountering human workers, they can potentially infer users' movements, routes, and identities. This cannot only reduce the acceptance of such solution, but also impacts their compliance with privacy legislation. Consequently, suitable solutions to protect users' privacy must be implemented.

This can be accomplished with a range of different location privacy-preserving techniques. One option is to report multiple false locations in addition to the user's actual position [7, 8, 16]. Thus, the user's location is hidden within the group of fake locations. However, this approach leads to a highly inefficient operation of AGVs because they cannot move within any of the reported areas. Another option is to apply *spatial cloaking* [14], i.e., the intentional reporting of inaccurate data, which we adopt in this work and evaluate its impact when applied in a smart factory setting. Spatial cloaking works

(a) Positions without spatial cloaking.

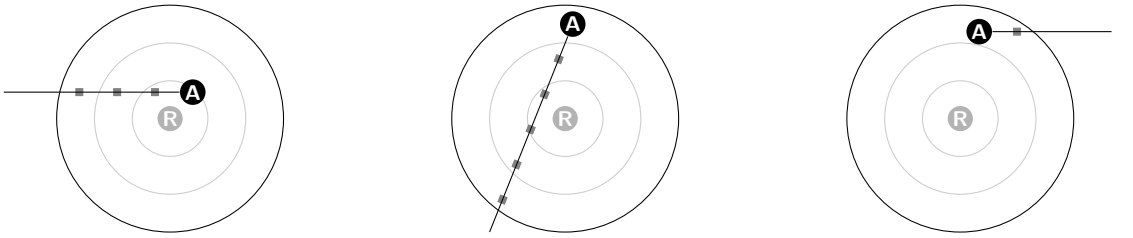
(b) Positions obfuscated by spatial cloaking.

Figure 6.3.1: Application of spatial cloaking to user position information.

as follows: A user's precise location is replaced by a representation of coarser spatial resolution. By way of example, let us look at the diagrams in Fig. 6.3.1. When users are required to report their exact positions in regular intervals (as shown in **??**), their trajectories can be easily traced. In contrast, when spatial cloaking is applied, falsified location points within a definable radius around the users' actual locations are being reported. This is visualized by means of the black markers in Fig. 6.3.1b. While these intentional deviations reduce the resolution at which a person can be tracked, they still appear as valid locations and often correctly describe a valid worker trajectory.

Spatial cloaking relies on two key parameters to determine the efficacy of its privacy protection: The radius of the reported area (depicted as a circle in Fig. 6.3.1) and the frequency at which reports are being sent. Frequent reporting rates and small reported radii lead to an accurate tracking of human workers, such that the likeliness of collisions with AGVs is greatly reduced. However, the attained degree of privacy protection is similarly low. Conversely, both larger reported radii and a reduced transmission frequency can be used to reduce the precision of the transmitted location information. The latter aspect, i.e., sending reports less frequently, also preserves the energy budgets of the smart wearables better.

However, a change of the reporting transmission frequency has a direct impact on workers' safety, as their actual positions are randomly distributed inside the reported area and unrelated to their heading direction. The risk ensues that workers leave the reported area in-between two successive transmissions, as the reported workers' location information remains the same until the next transmission. Thus, their protection against colliding with AGVs is no longer guaranteed. Fig. 6.3.2 illustrates three typical cases of reported locations (visualized by the light gray markers) with a radius of three. The worker's actual location is represented by the black markers, while the triangles illustrate the number of steps a worker can take without leaving the reported area and until the location have to be updated to ensure worker's safety. If we assume that the worker's actual location is close to the center of the reported area, the worker can take three steps in the given direction before he/she is leaving the reported area (see Fig. 6.3.2a). As the worker is unprotected after leaving the reported area, the location should be updated to ensure the worker's safety. If this is not the case, the worker is considered as unprotected until the next location transmission. In comparison, Fig. 6.3.2b illustrates the case when the workers' actual location is close to the perimeter of the reported area and the worker moves inwards. Here, the worker is protected for five steps before the worker leaves the reported area. Within the same transmission frequency as before, the worker is protected for a longer duration (i.e., more steps) in this case due to the actual location and the direction in which he/she moves. In contrast, the worker's actual location is also at an



(a) Location reported close to the center of the area.

(b) Location reported at area border, moving inwards.

(c) Location reported at area border, moving outwards.

Figure 6.3.2: Typical cases of location reporting for a cloaking radius of three; A is the worker's actual location and R the reported location. Triangles show the number of steps the worker can take without leaving the reported area.

area border in Fig. 6.3.2c, but the worker is moving outwards. The worker can only take one step within the same transmission frequency, in which he/she is protected by the reported area. Thus, changing the transmission frequency has an impact on the workers' safety depending on the worker's actual location and the direction he/she wants to move.

6.4 SIMULATION SETTINGS

The efficacy of spatial cloaking relies on the choice of its parameters. In order to assist in the choice of these parameters for the safe and efficient operation of workers and AGVs, we conduct an in-depth analysis of the parameter space. More specifically, we analyze how the following factors affect the accuracy of detection workers on a shop floor, and also assess the extent to which workers' privacy is preserved:

1. The maximum allowed deviation between actual and reported location, i.e., the *spatial cloaking radius*.
2. The location information transmission rate, i.e., the *spatial cloaking reporting frequency*.
3. The *transmission success rate* to take into account potential communication loss due to, e.g., channel contention or packet collisions.

For our analysis, we adopt the simulation environment described in Section 6.4.1. We further assume the behavior for both workers and AGVs as detailed in Sections 6.4.2 and 6.4.3, respectively. All simulation results show the average values of three runs with different random seeds.

6.4.1 *Simulation Environment*

To evaluate the different parameters, we have created a virtual simulation environment in NetLogo, an agent-based-social framework [25, 28]. In the simulation environment, our smart factory has a size of 128×64 meters (a square meter corresponds to a patch, which is the surface unit in NetLogo). Since factories are usually unique in size and organization [3, 9], we have chosen this particular setting to be able to get the first insights. An analysis of the impact of the factory organization on the results is foreseen

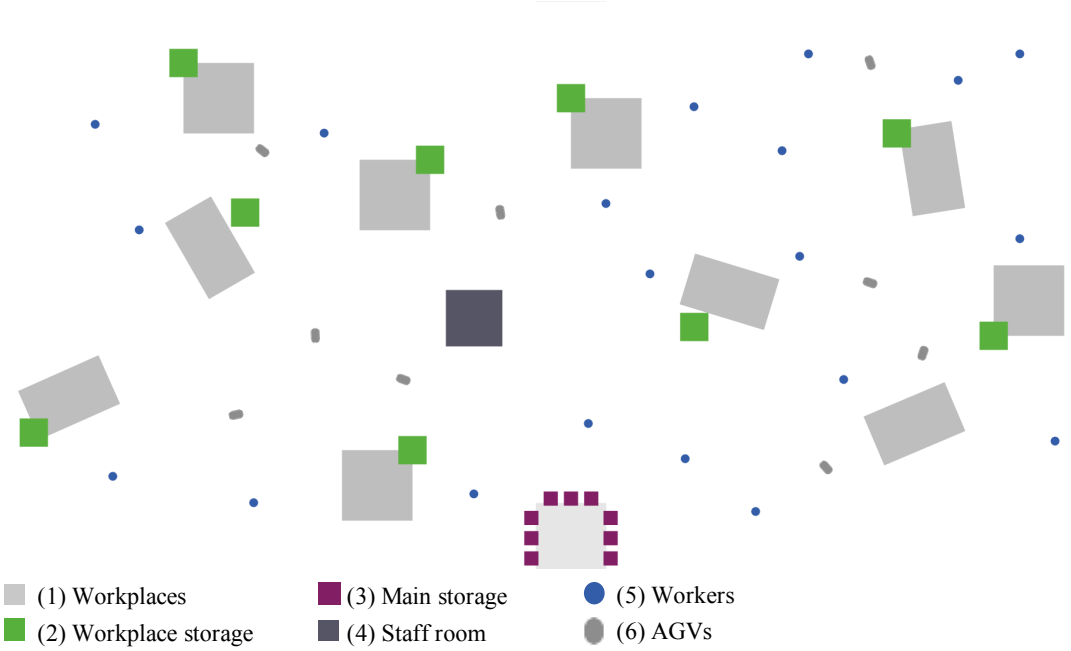
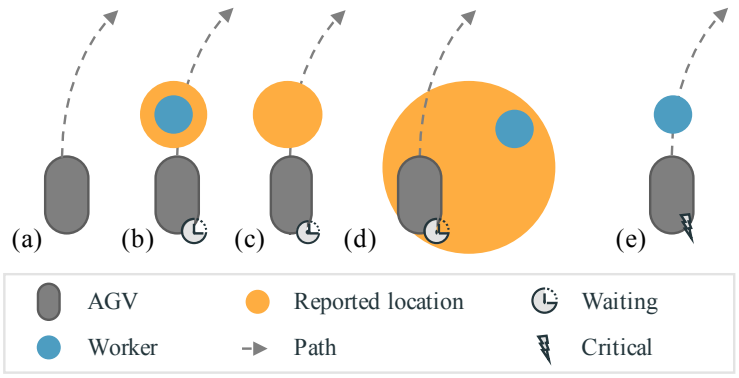


Figure 6.4.1: Sample arrangement of the smart factory used in our evaluation.

in future work. In this factory illustrated in Fig. 6.4.1, both workers and AGVs move between different areas. While workers visit both their workplaces and the staff room, AGVs roam between workplace storage units and the main storage room. This setting is applied to simulate a manufacturing setting, in which AGVs regularly deliver new materials to the workplaces and move completed items to the main storage. We set the number of workplaces to ten. By doing so, our simulated smart factory can accommodate multiple workers and AGVs with a meaningful degree of activity. During the initialization phase, workplaces are configured to have a pre-defined minimum distance to each other, such that both workers and AGVs are able to move between them easily. Additionally, this means that the trajectories of both AGVs and workers cross in different areas of the smart factory. We set the number of workers to 20 and the number of AGVs to nine. This ensures that each workplace storage is regularly visited by an AGV, and thus the AGVs are almost constantly in motion on the shop floor. Our simulations terminate when one of the following events occur: (1) when all workers had a near miss with AGVs, which arise when an AGV's and a worker's trajectories cross on the same patch at the same time or (2) when reaching the maximal duration of 36 000 seconds. All simulation settings are summarized in Table 6.4.1.

For each random seed, the workplaces, workplaces storages, staff room, AGVs, and workers are distributed randomly inside the factory environment. Only the main storage has a fixed location at the center of all simulated scenarios, as visible in Fig. 6.4.1. In order to fully explore the parameter space, we consider transmission success rates between 10 % and 100 % in increments of 10 %. Note that we have chosen this range of transmission rates to cover worst case scenarios, in which, e.g., workers' smart watches may be ill-functioning, and measure their impact on the workers' safety. We, however, expect a normal transmission success rate to be about 90 %. Likewise, we vary the size of the reported location between 0 (i.e., no spatial cloaking) and 15 meters around a worker. A further enlargement of the radius would only lead to longer AGV waiting times and thus



Figs. 6.4.2: Possible behaviors of AGVs.

to a significant reduction in productivity. We also vary the workers' location reporting frequency between 1 second and 20 seconds in increments of 1 second each. A further reduction of the frequency would only lead to an even shorter simulation duration and thus to lower workers' safety due to fewer location updates as explained in Section 6.3. This corresponds to a 10 h working day and thus approximately 2 h over the average working hours inside industrial environments. It hence provides a better comparison with real production environments [5, 26]. The previously introduced parameters are chosen to provide a good balance between the workers' and AGVs' motions.

6.4.2 *Worker Behavior*

We assume that workers move within the shop floor at a speed of 1.38 $\frac{\text{meters}}{\text{second}}$ between the staff room and the workplaces, as the average speed of a pedestrian is approximately 5 $\frac{\text{km}}{\text{h}}$ [4]. The length of stay of the workers at the workplaces and in the staff room is 1 second. This means that the workers are constantly in motion. At the moment a worker reaches the staff room, he/she selects a random free workplace to visit next. Each workplace can accommodate two workers. In this way it can be ensured that all workplaces in the shop floor are served. Thus, we can evaluate whether the workers' safety can be ensured despite the use of spatial cloaking. If an AGV's and a worker's trajectories cross on the same patch at the same time, the worker is considered to be in shock after this near miss with an AGV, so that he/she cannot work anymore until the end of the shift and is therefore not considered in the simulation scenario anymore. Each worker transmits his/her cloaked location via a smart wearable. This reported location depends on the spatial cloaking radius, the spatial cloaking frequency, and the transmission success rate, which are defined in Section 6.4.1.

6.4.3 *AGV Behavior*

We assume that AGVs move within the shop floor at a speed of 2.22 $\frac{\text{meters}}{\text{second}}$ between the main storages and the workplace storages. AGVs stay at their destinations for 1 second before continuing their journeys, so as to be constantly in motion. Fig. 6.4.2 illustrates the different AGVs' behaviors on the shop floor. An AGV follows its regular trajectory in absence of any workers' reported locations as shown in the first case, noted (a) in Fig. 6.4.2. An AGV immediately stops if it is about to enter a workers' reported location as

Table 6.4.1: Summary of the used simulation parameters.

Parameter	Value
Dimensions of the simulated scenario	128×64 patches
Number of workers	20
Number of AGVs	9
Number of workstations	10
Number of workstation storages	9
Worker velocity	1.38 $\frac{\text{meters}}{\text{second}}$
AGV velocity	2.22 $\frac{\text{meters}}{\text{second}}$
Maximum simulation duration	36 000 seconds
Transmission success probability	[0.1, . . . , 1.0]
Spatial cloaking radius	[0, . . . , 15] meters
Location transmission frequency	every $[1, \ldots, 20]^{\text{th}}$ second
Equivalent real-world distance per patch	1 m
Equivalent real-world time per interval	1 s

depicted in cases (b) and (c). In (b), the worker is still located in his/her reported location, while the worker already left the reported location in (c). The latter case can happen when the workers reduce their spatial cloaking reporting frequency. Otherwise, it is also possible that an AGV immediately stops, even if the worker does not cross their path as shown in case (d). When an AGV stops when entering a workers' reported location, it needs to wait until it is able to continue its trajectory. As a result, its productivity decreases. In the absence of workers' reported locations, the AGV continues its work even if a worker crosses its trajectory as seen in case (e). In this case, the AGV performs an emergency braking. We consider that this avoided collision may still fright the worker and impact his/her capacity to work. We hence consider that he/she is unable to work for the remaining of the shift. As a result, this worker is not considered in this simulation run anymore. Please note that this assumption is adopted to allow for an evaluation of the different parameters, and serves as the termination criterion for the evaluation.

6.5 SIMULATION RESULTS

We explore the sensitivity of spatial cloaking to the selected simulation settings summarized in Table 1. Across all evaluations, we use both the workers' safety and the AGVs' productivity as metrics. Since the simulation stops as soon as all workers have crossed the path of an AGV, we consider the simulation time as an indicator of the reached workers' safety: The longer the total simulation time, the better for the overall workers' safety. Likewise, the shorter the aggregated time during which AGVs are stopped, the higher the productivity.

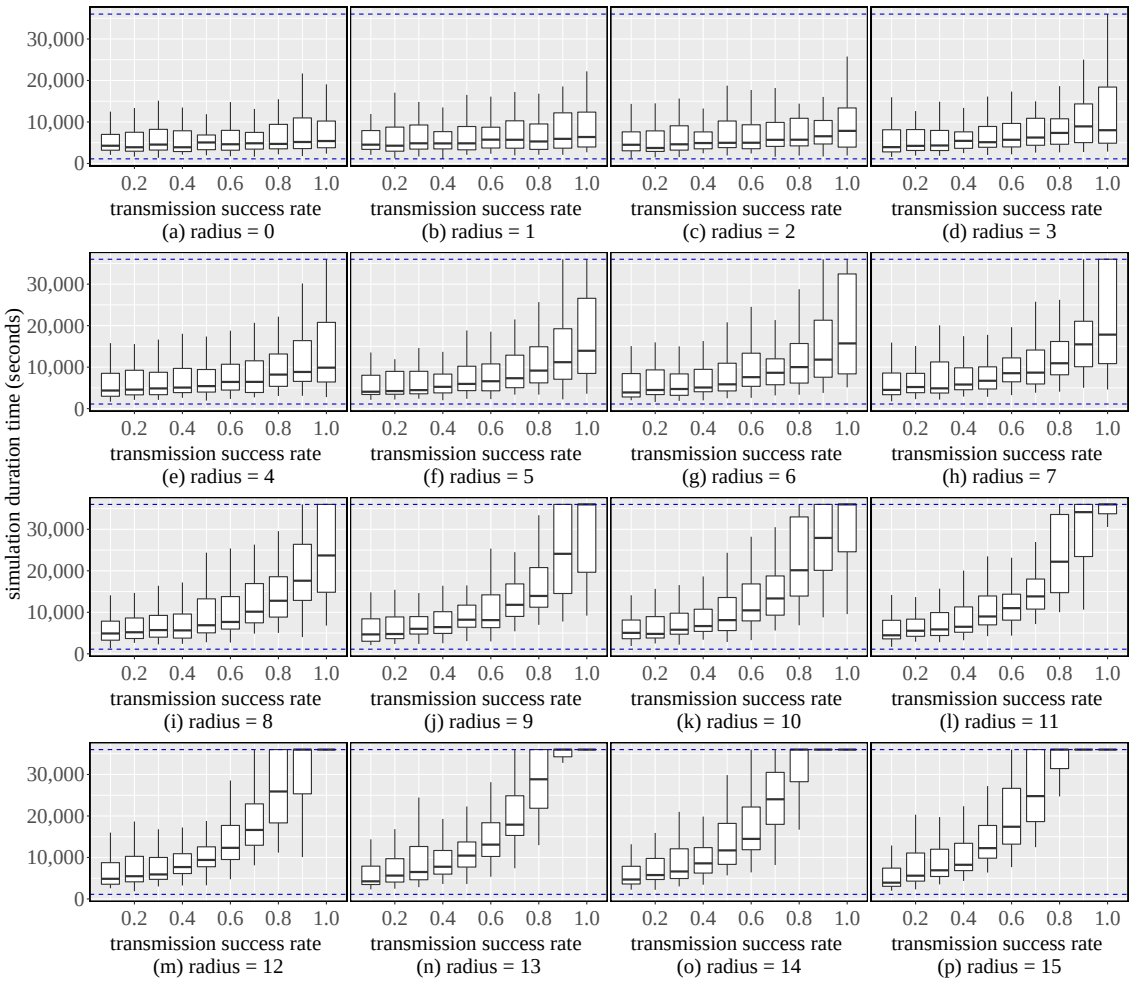


Figure 6.5.1: Influence of spatial cloaking radius on the workers' safety.

6.5.1 *Impact of the Spatial Cloaking Radius*

In our first evaluation, we investigate the influence of the spatial cloaking radius on both workers' safety and the AGVs' productivity. Intuitively, a larger radius leads to an increased location privacy protection for the workers and fewer near misses can happen between the AGVs and workers. However, this may decrease the AGVs' productivity.

Fig. 6.5.1 illustrates the results obtained when varying the spatial cloaking radius from 0 to 15 meters. A radius setting of 0 corresponds to reporting the exact workers' location, i.e., the baseline performance without spatial cloaking. In contrast, a radius of 15 corresponds to the most inaccurate location data reporting in our evaluation. The simulation duration is depicted along the y-axes of all box plots, with its upper limit of 36 000 seconds, as per Table 6.4.1. On the x-axis, different transmission success rate values are plotted. Boxes show upper and lower quartiles as well as the median value obtained for different values of the spatial cloaking radii. As expected, we observe that greater radii lead to better worker protection, which expresses itself through longer durations of the simulated settings, because each location report will stop all AGVs within the radius and near misses will thus be are avoided.

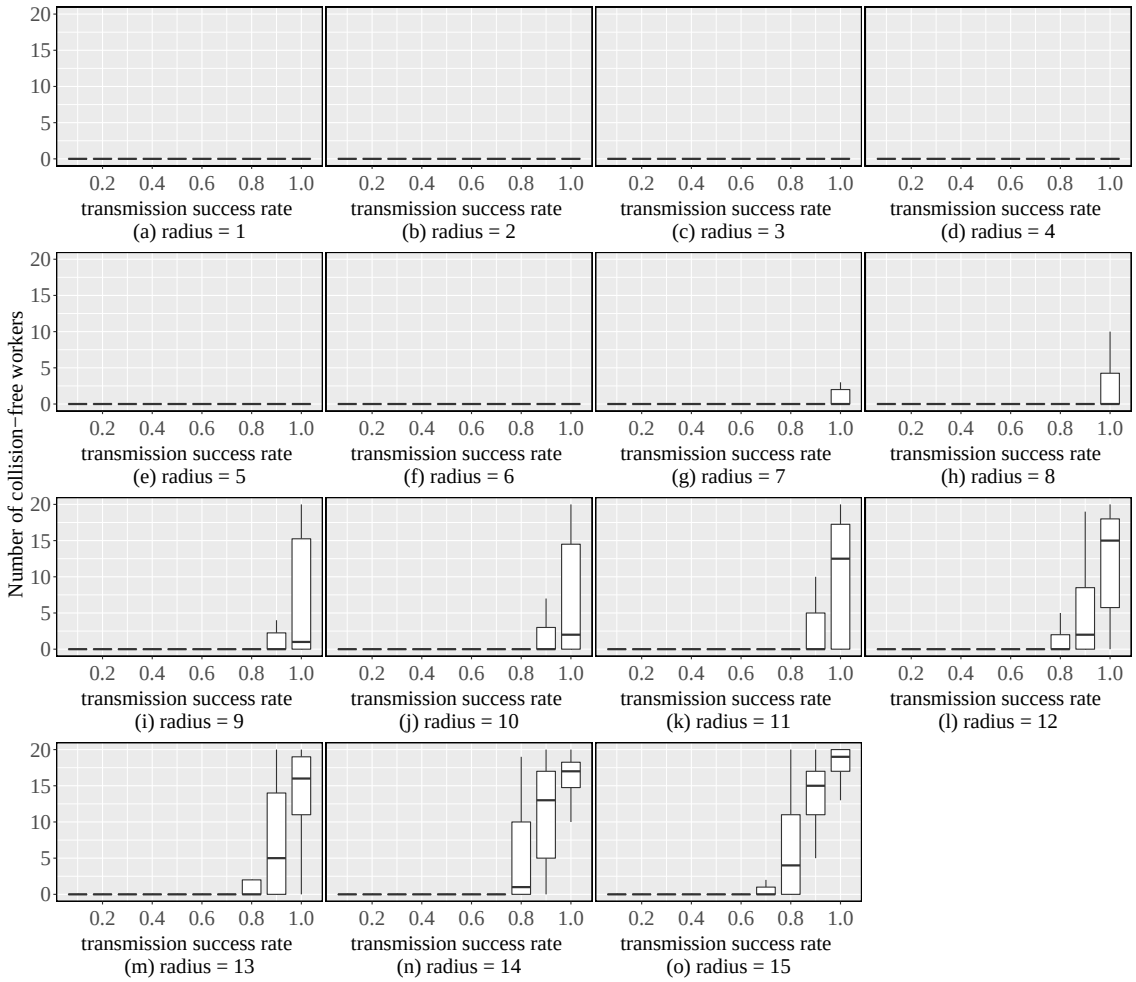


Figure 6.5.2: Influence of spatial cloaking radius on the number of collision-free workers.

A closer look reveals that the results for small radii show almost constant median values for the simulation duration regardless of the transmission success rate. This indicates that spatial cloaking with small radii leads to many near-misses between workers and AGVs. In contrast, increasing the spatial cloaking radius improves the workers' safety. From a radius of 9 meters, the median simulation duration is 36 000 seconds, i.e., the full simulation duration. As expected, the simulations confirm that transmission success rate has an impact on the workers' safety. For the same radius of 9 meters, packet losses of just 10 % lead to a 17 % decrease of the simulation duration. Moreover, the medians reveal that the last four radii in the highest transmission success rate reached the full simulation duration. Likewise, the last two radii reached the full simulation duration, also with a 90 % transmission success rate. It becomes apparent that the simulation results are sensitive to the transmission success rate. Four more workers remain active (i.e., have not experience near misses with an AGV) when a transmission success rate of 100 % is assumed instead of 90 %, for a radius of 15 meters. When using smaller radii, an even greater number of workers remains collision-free until the end of the simulation duration (11 for a radius of 13 meters, 8 for a radius of 14 meters) when assuming a transmission success rate of 100 %.

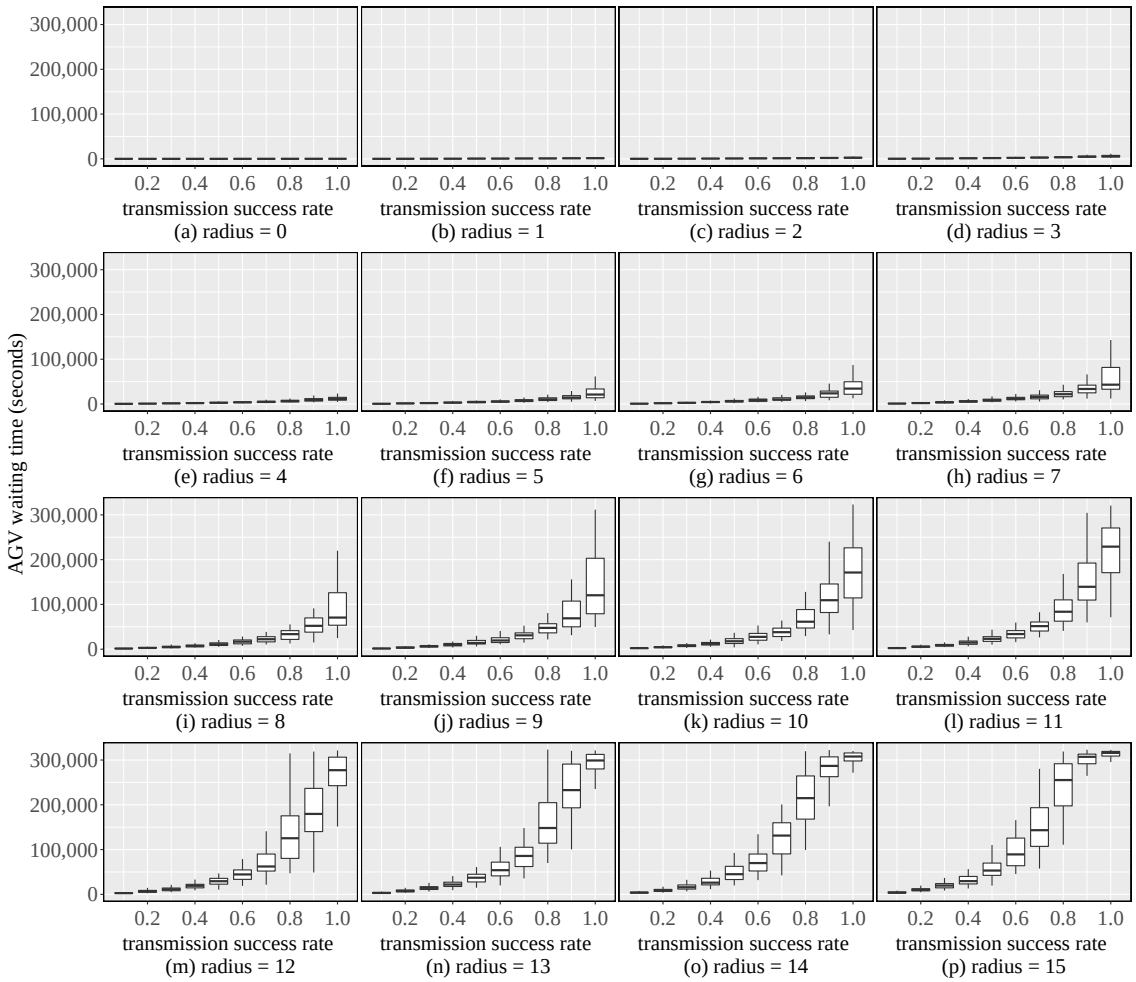


Figure 6.5.3: Influence of the spatial cloaking radius on the AGVs' productivity.

Fig. 6.5.3 illustrates the influence of the spatial cloaking radius on the AGVs' aggregated waiting time for different transmission success rates. As expected, smaller radii especially for higher transmission success rates lead to higher AGVs' productivity, as the AGVs wait significantly less time. For example, assuming no packet losses, the nine AGVs only need to wait for a total of 3 min for a spatial cloaking radius of 0 meters. This time drastically increases to 28 h 21 min when using a radius of 9 meters, and 78 h 54 min for 15 meters in total. For a very lossy link with an assumed transmission success rate of only 10 %, the AGVs' waiting time increase by 61 % when the spatial cloaking radius increases from 9 meters to 15 meters, so that the AGVs seem to stand still almost continuously for larger radii. This confirms the expected trade-off between the size of the spatial cloaking radius for the worker's safety and the AGV's productivity.

6.5.2 *Impact of the Spatial Cloaking Reporting Frequency*

We further analyze the effect of the spatial cloaking reporting frequency on both workers' safety and AGVs' productivity. We assume that a more frequent reporting would lead to an increase of the AGVs' productivity. Moreover, it should lead to fewer near misses between AGVs and workers. However, since their cloaked locations are reported more

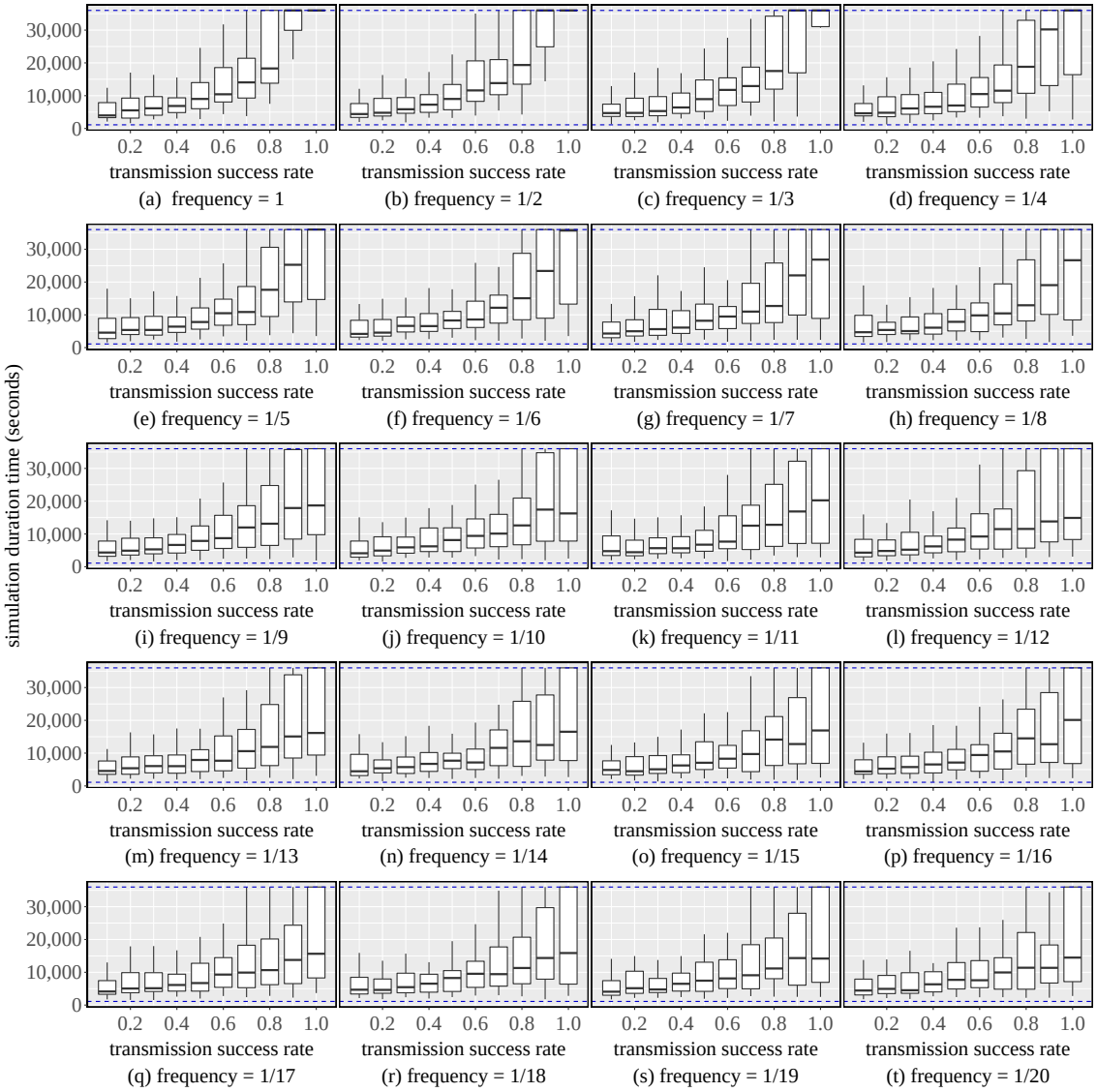


Figure 6.5.4: Influence of spatial cloaking frequency on the workers' safety.

often, it may be easier for an attacker to infer the workers' actual locations from the reported ones. Fig. 6.5.4 illustrates the obtained results for spatial cloaking frequency ranging from 1 to 20 seconds. As expected, we observe that higher frequencies lead to a better workplace safety, as expressed through a longer simulation duration and thus to increased workers' safety. In fact, frequent location updates allow the AGVs to avoid collisions. The graphs indicate that the median values in lower transmission success rates are almost constant. In comparison, for higher transmission success rates and higher reporting frequencies, the simulation duration tend to reach the full simulation duration time of 36 000 seconds. This indicates reporting that spatial cloaking with longer frequencies leads in many cases to unprotected workers, and hence more near misses occur, as the workers take out of their reported locations and are therefore unprotected, until their next location update. From a frequency of 6 seconds, the median simulation duration achieved is equal to the maximum simulation duration on lossless wireless channels. However, the next lower frequency of 7 seconds in-between transmissions leads

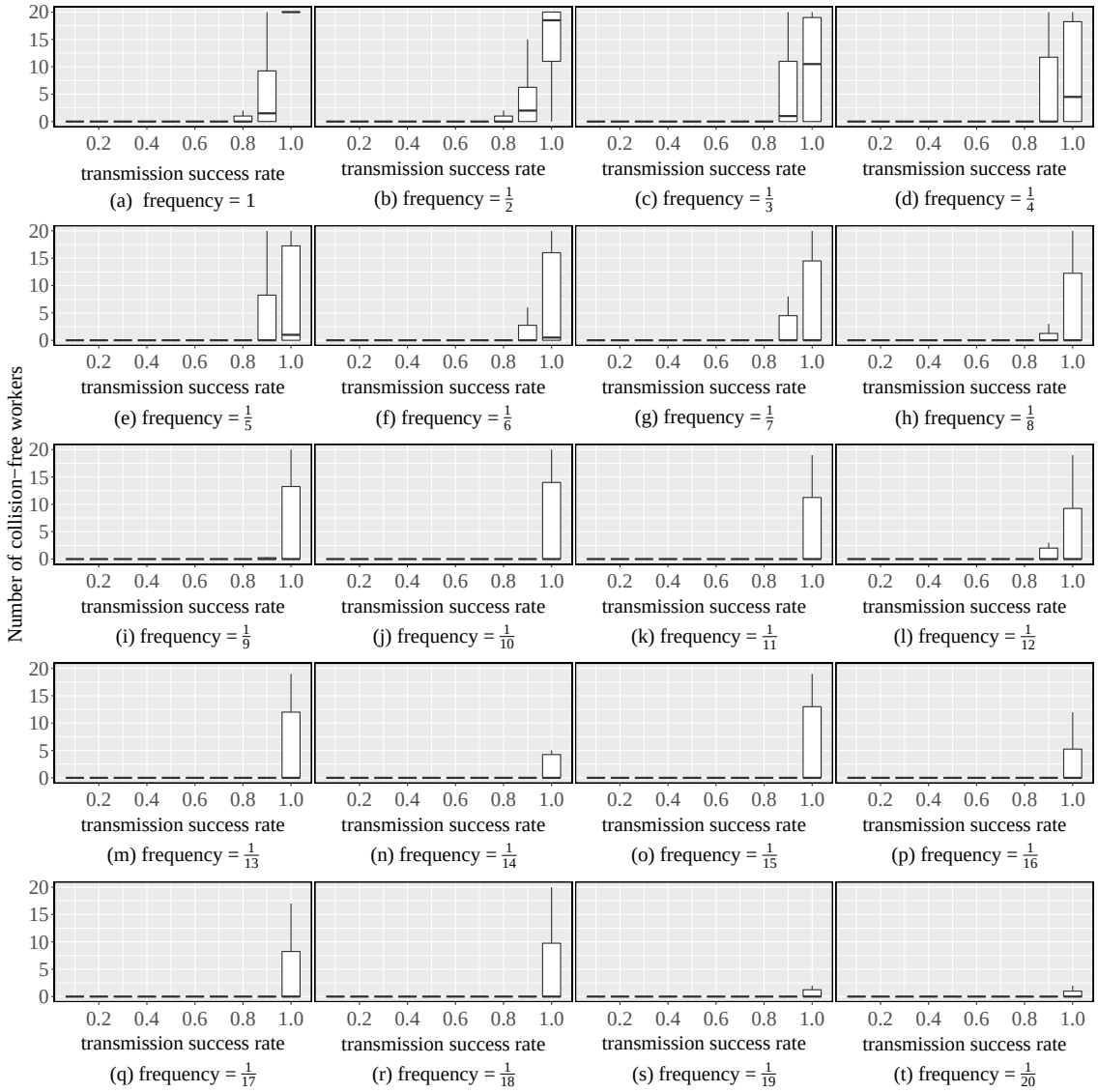


Figure 6.5.5: Influence of spatial cloaking frequency on the number of collision-free workers.

to a reduction of the median simulation duration time by 34.16 %, and thus to less workers' safety. Moreover, the results of lower frequencies, especially in conjunction with high transmission success rates, indicate a greater variance. The reason for this is due to the effects of the radius settings, as larger radii increase the workers' safety, especially when using lower reporting frequencies. Workers in small radii leave their protection zones significantly faster, which means that they are unprotected for a certain period of time, as mentioned in Section 6.3. For example, at a frequency of 5 seconds with a radius of 15 meters, no worker experiences a near miss with an AGV. However, at the same frequency, but with a reduced radius to 10 meters, just 10 workers reached the full simulation duration. While with a further reduction, to a radius of 5 meters, no worker is collision-free anymore. In addition, Fig. 6.5.5 demonstrates the influence of spatial cloaking frequency on the number of collision-free workers for different transmission success rates. In particular, the change in-between a frequency of 1 and 3 seconds without any transmission losses lead to 9.5 additional near misses between workers and AGVs

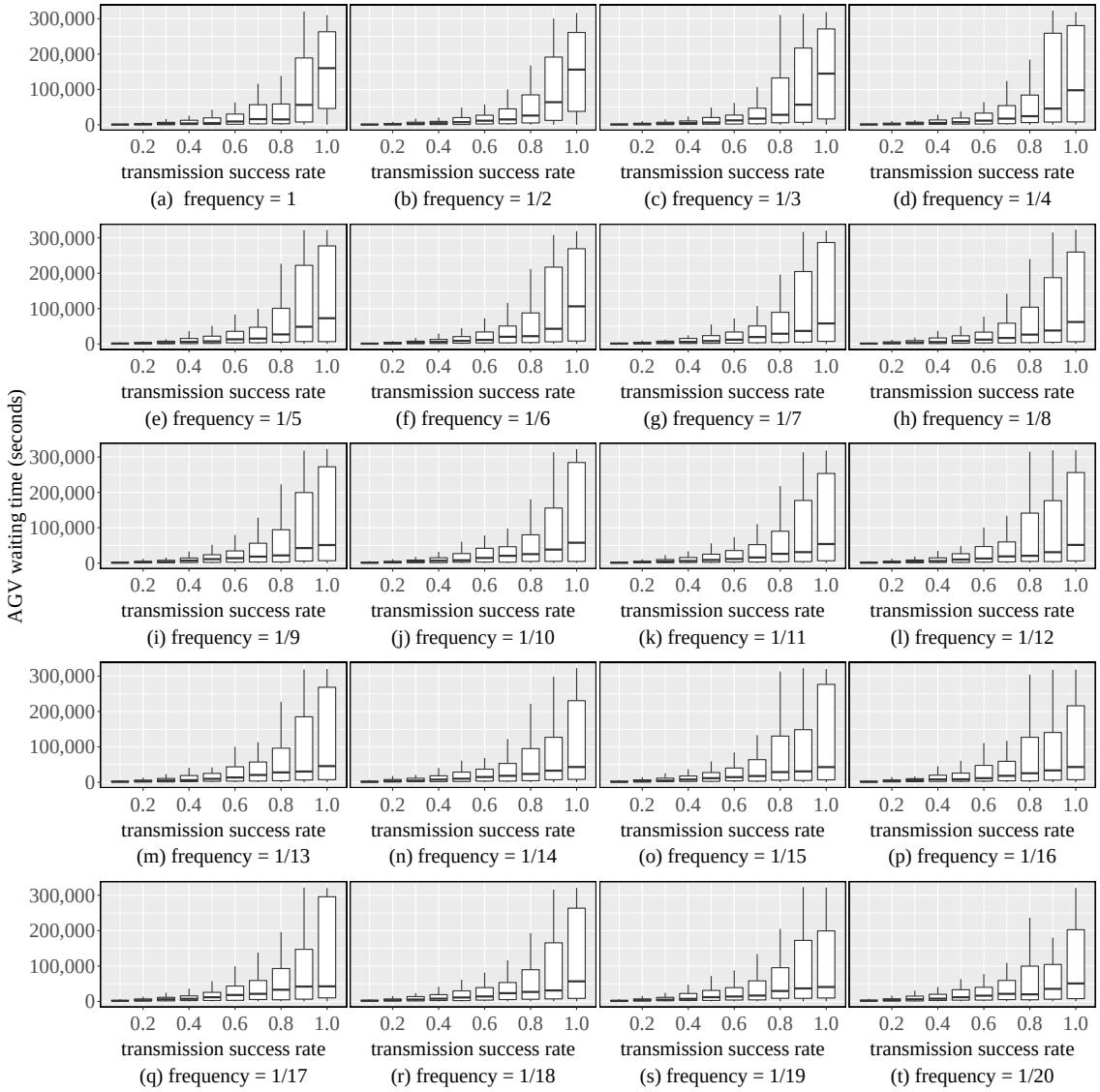


Figure 6.5.6: Influence of spatial cloaking frequency on the AGVs' productivity.

in average. Remarkably, even a 10 % signal loss lead also in the transmission frequency of 1 second immediately to worse workers' safety as only 1.5 workers achieved the full simulation duration time.

At last, Fig. 6.5.6 illustrates the influence of the spatial cloaking frequency on AGVs' productivity. We observe that the AGVs' waiting times increase slightly when using more frequent location transmissions, especially for higher transmission success rates. The longer AGVs' waiting times can be attributed to the fact that the AGVs have to stop more often when workers' location updates (with randomness added through spatial cloaking) are received more frequently.

6.5.3 *Limitations*

This paper aims to gain insights about privacy-preserving human-machine co-existence on smart factory shop floors. Our results have, however, three main limitations described

in what follows. Firstly, our results are based on the factory settings we have chosen. Since these settings can highly vary between factories [3], a common factory model to cover all scenarios is almost impossible to establish. As a result, our results cannot be generalized to all factories at this stage. They, however, lay the ground for gaining preliminary insights about the feasibility of our approach and we plan to investigate the impact of the factory layout on the obtained results in future work. Secondly, we assume in our simulations that the AGVs are only able to locate workers based on the location information provided by their smart watches. However, in case of near misses, the AGVs are able to perform emergency brakings, so that workers will not be injured. Therefore, in a real-world scenario, the AGVs would likewise be equipped with additional sensors to cater for redundancy and thus, ensure workers' safety if their devices should stop working or to prevent near misses in advance. The third and last limitation of this paper is that the privacy protection offered by spatial cloaking has not been directly measured in our simulations, as our primary focus is to first determine whether and under what conditions the suggested approach is feasible with regards to workers' safety. A detailed analysis of the privacy protection offered by this approach based on different attacker models is planned in future work, though.

6.6 CONCLUSION AND OUTLOOK

In this paper, we have considered the co-existence of workers and AGVs on smart factory shop floors. Through smart wearable devices configured to regularly transmit position announcements of the human workers, collisions between workers and AGVs can be avoided. Transmitting workers' location information, however, threatens their privacy. We have therefore applied a privacy-preserving solution and measured its effects on both the AGVs' productivity and the resulting workers' safety by means of simulations. While our results are restricted to our tested scenario, they confirm our expectations and allow to quantify the effects of the tested parameters, i.e., the reporting radius, its frequency, as well as the transmission success rate. The results show that the larger the cloaking radii are selected, the better it is for the workers' safety. However, larger radii imply a significant reduction in the AGVs' productivity, which may not be compatible with a real-world deployment. Furthermore, to enhance workers' safety in real-world industrial environments, the AGVs could use previous workers' locations until a new one has been transmitted. Therefore, our work lays the foundation for future explorations of different privacy-preserving solutions. Preserving privacy may help companies to convince workers and works councils to use smart wearables to exploit this potential. Nevertheless, we believe that future research on other location privacy techniques and attacker models is required to fully realize privacy-preserving smart factory environments.

REFERENCES

[1] ABI Research. *ABI Research Forecasts Enterprise Wearables will Top US$60 Billion in Revenue in 2022*. 2017. URL: Online:https://www.abiresearch.com/press/abi-research-forecasts-enterprise-wearables-will/ (visited on 06/29/2019).

[2] L. Bao and S. S. Intille. "Activity Recognition from User-Annotated Acceleration Data." In: *Pervasive Computing*. Ed. by T. Kanade et al. Vol. 3001. Lecture notes in computer science. Springer Berlin Heidelberg, 2004.

[3] S. Benjaafar, S. S. Heragu, and S. A. Irani. "Next Generation Factory Layouts: Research Challenges and Recent Progress." In: *Interfaces* 32.6 (2002).

[4] N. Carey. *Establishing Pedestrian Walking Speeds*. Tech. rep. Portland State University, 2005.

[5] M. Carley. *Working Time Developments – 2008*. 2009. URL: Online:https://www.eurofound.europa.eu/publications/report/2009/working-time-developments-2008 (visited on 07/12/2019).

[6] B. Choi, S. Hwang, and S. H. Lee. "What drives Construction Workers' Acceptance of Wearable Technologies in the Workplace?: Indoor Localization and Wearable Health Devices for Occupational Safety and Health." In: *Automation in Construction* 84 (2017).

[7] C.-Y. Chow, M. F. Mokbel, and W. G. Aref. "Casper*: Query Processing for Location Services without Compromising Privacy." In: *ACM Transactions on Database Systems (TODS)* 34.4 (2009).

[8] C.-Y. Chow, M. F. Mokbel, and X. Liu. "Spatial Cloaking for Anonymous Location-Based Services in Mobile Peer-To-Peer Environments." In: *GeoInformatica* 15.2 (2011).

[9] A. Drira, H. Pierreval, and S. Hajri-Gabouj. "Facility Layout Problems: A Survey." In: *Annual reviews in control* 31.2 (2007).

[10] H. Golnabi. "Role of Laser Sensor Systems in Automation and Flexible Manufacturing." In: *Robotics and Computer-Integrated Manufacturing* 19.1-2 (2003).

[11] N. Gorm. "Personal Health Tracking Technologies in Practice." In: *Companion of the ACM Conference on Computer Supported Cooperative Work and Social Computing (CSCW)*. Ed. by C. P. Lee, S. Poltrock, L. Barkhuus, M. Borges, and W. Kellogg. 2017.

[12] N. Gorm and I. Shklovski. "Sharing Steps in the Workplace." In: *Proc. of the ACM Conference on Human Factors in Computing Systems (CHI)*. 2016.

[13] A. Grau, M. Indri, L. L. Bello, and T. Sauter. "Industrial Robotics in Factory Automation: From the Early Stage to the Internet of Things." In: *Proc. of the 43rd Annual Conference of the IEEE Industrial Electronics Society (IECON)*. 2017.

[14] G. D. Gruteser M. "Anonymous Usage of Location-based Services Through Spatial and Temporal Cloaking." In: *Proc. of the 1st International Conference on Mobile Systems, Applications, and Services (MobiSys)*. 2003.

[15] C. Ilas. "Electronic Sensing Technologies for Autonomous Ground Vehicles: A Review." In: *Proc. of the 8th International Symposium on Advanced Topics in Electrical Engineering (ATEE)*. 2013.

[16] H. Kido, Y. Yanagisawa, and T. Satoh. "An Anonymous Communication Technique using Dummies for Location-based Services." In: *Proc. of the 2nd International Conference on Pervasive Services (ICPS)*. 2005.

[17] S. W. Lee and K. Mase. "Activity and Location Recognition using Wearable Sensors." In: *IEEE Pervasive Computing* 1.3 (2002).

[18] E. Lingg, G. Leone, K. Spaulding, and R. B'Far. "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)*. 2014.

[19] D. Lucke, C. Constantinescu, and E. Westkämper. "Smart Factory-A Step Towards the Next Generation of Manufacturing." In: *Manufacturing Systems and Technologies for the New Frontier*. Springer, 2008.

[20] A. Murphy. *AGV Deep Dive: How Amazon's 2012 Acquisition Sparked a $10B Market*. (accessed: 2019-06-29). Aug. 10, 2017. URL: Online:https://loupventures.com/agv-deep-dive-how-amazons-2012-acquisition-sparked-a-10b-market/.

[21] M. Peissner and C. Hipp. *Potenziale der Mensch-Technik-Interaktion für die effiziente und vernetzte Produktion von morgen*. Fraunhofer-Verlag Stuttgart, 2013.

[22] A. Radziwon, A. Bilberg, M. Bogers, and E. S. Madsen. "The Smart Factory: Exploring Adaptive and Flexible Manufacturing Solutions." In: *Procedia engineering* 69 (2014).

[23] V. Schellewald, B. Weber, R. Ellegast, D. Friemert, and U. Hartmann. "Einsatz von Wearables zur Erfassung der körperlichen Aktivität am Arbeitsplatz." In: *DGUV Forum* 11 (2016).

[24] A. Stocker, P. Brandl, R. Michalczuk, and M. Rosenberger. "Mensch-zentrierte IKT-Lösungen in einer Smart Factory." In: *e & i Elektrotechnik und Informationstechnik* 131.7 (2014).

[25] S. Tisue and U. Wilensky. "NetLogo: A Simple Environment for Modeling Complexity." In: *Proc. of the 7th International Conference on Complex Systems (ICCS)*. 2004.

[26] U.S. Bureau of Labor Statistics. *Average Weekly Hours of All Employees: Manufacturing [AWHAEMAN]*. 2019. URL: Online:https://fred.stlouisfed.org/series/AWHAEMAN (visited on 07/12/2019).

[27] M. Weston. "Wearable Surveillance – A Step too far?" In: *Strategic HR Review* 14.6 (2015). ISSN: 1475-4398.

[28] U. Wilensky, E. Hazzard, and R. Froemke. "GasLab: An Extensible Modeling Toolkit for Exploring Statistical Mechanics." In: *Proc. of the 7th European Logo Conference (EUROLOGO)*. 1999.

[29] J.-S. Yoon, S.-J. Shin, and S.-H. Suh. "A Conceptual Framework for the Ubiquitous Factory." In: *International Journal of Production Research* 50.8 (2012).

[30] Zebra Technologies. *Zebra Study Reveals One-Half of Manufacturers Globally to Adopt Wearable Tech by 2022*. June 31, 2017. URL: Online:https://www.zebra.com/us/en/about-zebra/newsroom/press-releases/2017/zebra-study-reveals-one-half-of-manufacturers-globally-to-adopt-.html (visited on 06/29/2019).

7

SUMMARIZED CONTRIBUTIONS

This section highlights our contributions that answering our research questions introduced in Section 1.3. We further summarize their implications and comment on their limitations.

7.1 SUMMARIZED ANSWERS TO THE RESEARCH QUESTIONS

RQ 1: Which employees' level of knowledge regarding privacy risks results in acceptance problems?

Our first research question was answered in Paper II. It explores the impacts of employees' legislation knowledge, technical knowledge about smart watch capabilities, and technical affinity on their willingness to share such information. In addition, Paper II investigates whether smart watch ownership and usage correlate with this willingness. Note that the unwillingness to share such private data with the employer is associated with resulting acceptance problems.

Based on the obtained results, the employees' knowledge of both technical and legislation impacts employees' willingness to share private data collected by smart watches. The results show that a majority of our participants are aware of what can be processed and used with the data collected by a smart watch. For example, most of them know that these data can be used to draw inferences about their health. Employees have, however, partially incorrect knowledge about legal frameworks, especially about collective agreements and the GDPR purposes. The results indicate that half of our participants know what personal data are, while the other half answered incorrectly or indicated not to know. Besides, the majority indicated that collective agreements are not a permissible form of agreement to collect and use employees' data. Furthermore, most of them do not know that a collective agreement can replace a person's consent. Apart from that, this willingness is also affected by other important factors like technical affinity or ownership. Our results reveal that the ownership of a personal smart watch leads to differences in their willingness to share data, as does the employees' technical affinity. Besides, among the different data types considered in Paper II, the participants were more reluctant to share health data than activity or location data.

- **All in all**, the acceptance of smart watches is not only related to privacy risks, as the results indicate further factors that have an impact on it. Hence, employees' knowledge regarding the technical capabilities of a

smart watch or their understanding of legislation regulations affects their acceptance in the sense of their willingness to share private data with their employer.

RQ 2: Which information or conditions influence employees' acceptance?

Paper III answer indirectly our research question 2 by answering research question 2.1 and research question 2.2. Paper III investigates the impact of employers' provided information on employees' willingness to share private data with their employers by modifying the information provided with more information about benefits and risks.

RQ 2.1: Does more extensive information provided to the employees increase their willingness to disclose private information to their employer?

Extending the information provided by the employer about smart watches is not expected to increase employees' willingness to share private data. The results in Paper III reveal that our participants' intention to disclose private data to their employer decreased when providing more information regarding smart watch benefits and risks. Therefore, more detailed information concerning the benefits and risks when using smart watches led to a decrease in employees' willingness to share private data with their employer. Employees may weigh privacy risks higher than benefits, especially because these risks, when they occur, are more noticeable than in the private context.

RQ 2.2: How does the provision of more extensive information influence the relationship between perceived risk, benefits, and the intention to disclose information?

The obtained results in Paper III partially confirm that 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. The results indicate that 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.

Hence, employees give greater weight to their perceived risks after being provided with more information.

- **In summary**, the findings show that merely because employers increase the information provided about the benefits and risks associated with smart watches, employees are not influenced in their acceptance of sharing personal data collected with a smart watch. On the contrary, simply providing more information tended to make employees more aware of the risks and thus more likely to refuse to share their private data.

RQ 3: How do solutions need to be implemented in companies to ensure and enhance employees' privacy?

Paper IV and V answer this research question. While Paper V explored a privacy-preserving solution, Paper IV examined a TET on a smart watch, when collecting private data. Paper IV refers directly to sub research questions 3.1 and 3.2 and thus can only indirectly answer research question 3. Likewise, Paper V refers only to the sub research question 3.3. The sub research questions are the following:

RQ 3.1: Which transparency indicator visualization(s) do employees perceive as sufficient and useful to be informed about the current data collection?

The results in Paper IV reveal that our participants prefer the splash-screen design (see Fig. 7.1.1a). This design requires an additional and active action from the users to access the watch's main screen. In contrast, both other designs do not require a dedicated interaction from the users. However, the differences in terms of preferences between the splash-screen design and the other designs remain low. In addition to such visual elements, the results indicate that participants' opinions differ regarding additional feedback, either sound or vibrations. Apart from that, our results suggest that most would not deactivate such privacy indicators, which highlights that they would like to know when data collection arises. Thus, employers should implement privacy indicators.

(a) Splash-screen design (b) Circular design (c) Icon design

Figure 7.1.1: Examples of proposed indicators to visualize the collection of health data on a smart watch

As employees slightly differ in their needs, employers could let employees choose from different indicators according to their preferences for indicators, additional feedback, or even the deactivation of the privacy indicator.

RQ 3.2: Which interaction(s) is/are perceived by the employees as appropriate to control the data collection?

The results in Paper IV, suggest that our participants want to have the control to interrupt employers' data collection when working with a smart watch. Especially in situations considered as private including private conversations, breaks, or going to the toilet. Such function can be done by different control interactions. The results indicate that our participants prefer to press a button in the menu or interact with a physical button on the smart watch to stop the data collection. Hence, employees would like to have discrete interactions.

As indicated Paper V answered the following sub research question:

RQ 3.3: What trade-off exists between employee workplace safety and AGVs' productivity?

Our simulations in Paper V of the privacy-preserving solution spatial cloaking allowed us to measure the effects of the cloaking on both the AGVs' productivity and the resulting workers' safety. Our tested scenario quantifies the impact of the tested parameters, i.e., the reporting radius, frequency, and transmission success rate. The results show that the larger the cloaking radii are selected, the better it is for the workers' safety. However, larger radii imply a significant reduction in the AGVs' productivity. In other words, the productivity of the AGVs will decrease if the employer decides to use the solution with the most privacy-friendly conditions for its employees. Hence, both can not be achieved to a high degree. Moreover, to achieve better workplace safety employees current locations have to be updated more

frequently. With higher frequencies AGVs have more reliable location data and thus avoid collisions. Consequently, employees must accept privacy limitations, or further research with other environments or other privacy-preserving solutions is needed.

- **In summary**, the results for the two research questions 3.1 and 3.2 indicate that different indicators and interactions are conceivable for employees. However, our results show tendencies for specific indicators and interactions. Most prefer the splash-screen design as a privacy indicator and pressing a button in the menu or a smart watch physical button to stop the data collection. In addition to the visual elements, employees should be able to add additional feedback (sound or vibration) on the smart watch or even deactivate the privacy indicator. Finally, both sub research questions answer our research question 3 by offering a solution that improves employee privacy through enhanced transparency and control.

  Apart from this, the result for the last remaining research question 3.3 indicates that the implementation of spatial cloaking on the transmitted employees' locations as a solution, which fits all interest of both employers and employees, is not efficient. The productivity of the AGVs decreases if employers implement spatial cloaking with high privacy-preserving conditions for employees. Both cannot be achieved to a high degree. In consequence, employees would have to accept privacy restrictions to achieve higher AGVs' productivity, which would be in the interest of their employers. Finally, this sub research question answers our research question 3 by testing the effects of a privacy solution simulated in a company environment.

7.2 IMPLICATIONS

Our results have the following implications considering the different steps of smart watch deployments in smart workplaces introduced in Section 1.4. These implications serve both scientific research as well as in operational practice. Although our implications serve scientific research in filling research gaps, this thesis mainly supports employers in understanding employees' knowledge, behavior, and preferences when considering a smart watch deployment. Hence, from the practice perspective, the lesson learned in our research are the basis for the following recommendations for employers to enhance employees' privacy from different perspectives.

1. **Before the planned smart watch introduction**

   We found that different factors impact the employees' willingness to share personal data with their employers. These factors are employees' legislation knowledge, technical affinity, and smart watch ownership. Moreover, based on our findings, we assume that employees' technical knowledge about the smart watch' capabilities indicates their awareness of a smart watch' technical possibilities. Hence, this technological knowledge may negatively influence employees' decisions to accept

a smart watch at work, as they perceive it and the associated data collection negatively.

- Thus, we recommend that employers consider employees' knowledge about smart watches and legislation frameworks when implementing smart watches to reduce potential misunderstandings about the data to be collected. Likewise, they should provide transparency about the collected data and apply adequate privacy-preserving mechanisms. Furthermore, employers should clarify the exact process from planning to integrating smart watches in their processes and which and where related information is available to employees. Moreover, employers should develop methods, such as trainings, to bridge potential employees' knowledge gaps.

2. **During the introduction of smart watches**

   We found that employers cannot easily expand the information provided by employers by including more information about the benefits and risks associated with smart watches so that employees are willing to share data with employers. Consequently, providing more information leads to an increase in employees' risk awareness and, therefore, they are less likely to share their private information collected with the smart watch. As a result, providing more information about benefits and privacy risks side by side is insufficient.

   - Thus, we recommend employers not to just extend the provided information associated with smart watch risks and benefits. They should provide more comprehensive information about the smart watch introduction in their companies, and should simultaneously provide privacy solutions to mitigate privacy risks. Employers should consider this aspect, even if a generational change in the workforce could lead employees to be more open to smart technologies and data disclosure in the long term, as we found, that younger people tend to be more familiar with the benefits of smart devices and may perceive privacy risks differently. Contrary, employees could be more aware of the risks that might occur due to the employee-employer relationship and, therefore, unwilling to share such data with their employers in the future. Besides, we recommend that employers should never force their employees to accept any new technology able to collect sensitive data, as voluntary use may increase the effectiveness and satisfaction of the employees.

3. **During smart watch use** and data collection

   First, we found that employees prefer a privacy indicator and smart watch interaction, which are more familiar to them. For privacy indicators, employees chose our proposed splash-screen design, which informs the smart watch wearer about current data collection like a usual notification on the smart watch display. Moreover, we found that some employees would like to add additional feedback like sound and vibrations. Besides, we found that employees would like to deactivate smart watch data collection, especially in private situations. For this, employees would prefer to press a virtual button in a menu or a physical button on the smart watch frame. Hence, both interactions are thus more common smart watch interactions than gestures like twisting the arm.

- Therefore, we recommend that employers should implement valuable privacy indicators and interactions to allow employees to stop data collection temporarily. As our results of the proposed privacy indicators differ slightly, we suggest employers should let employees choose from different indicators according to their preferences. Likewise, the use of supplementary feedback like sounds or vibration should be an option. Hence, employers should support individuals' preferences and offer different options. However, we recommend considering employees' working environments to evaluate potential safety issues that might arise if they are distracted by a sound or vibration notification during their tasks. Beside, some employees might like to disable such indicator. We recommend employers to let them disable it when they want to, as it was not intended to be distracting. Regarding the interactions to stop data collection, we recommend employers to provide discrete interactions to allow employees to stop the data collection especially in privacy-sensitive situations.

Finally, we found that the deployment of the privacy-preserving mechanism spatial cloaking to cloak employees current location is insufficient when concerning workplace safety and AGVs' productivity. As larger cloak radii imply a significant reduction in the AGVs' productivity, which may not be compatible with a real-world deployment. Moreover, we observe that higher frequencies lead to a better workplace safety, as the AGVs receive employees' current location more frequently. Hence, frequent location updates are more reliable and allow the AGVs to avoid collisions.

- Thus, we recommend employers to consider our research findings even if our workplace setting in our simulations remains general. Employers must find the best parameters for each factor for their smart workplaces to achieve workplace safety and AGVs productivity. Furthermore, to enhance workers' safety in real-world industrial environments, the AGVs could use previous workers' locations until a new one has been transmitted. However, note that the privacy protection offered by spatial cloaking has not been directly measured in our simulations, as our primary focus is to first determine whether and under what conditions the suggested approach is feasible with regards to workers' safety. Apart from this, employers must take a works council (if any) in on the action to elaborate on the best solution for employees.

7.2.1 *Limitations*

Alongside with our contribution to the research, we acknowledge the following limitations:

1. The insights of this thesis are mostly based on online questionnaires, which may not be directly applicable to the real-world, as the answers provided by our participants reflect their claimed opinions and not necessarily their actual behavior. However, we focused on full-time employees to mitigate such limitations, as they have usually different opinions than other socio-demographic groups.
2. We focus on full-time employees in Germany and over 18. Hence, the obtained results may differ for other cultures and younger employees.

3. Our questionnaires are based on hypothetical scenarios that participants needed to imagine. As a result, they may not have fully connected the given scenario with their own work. Moreover, we did not classify in advance, which kind of workplace a participant has to work in to participate. Participants may have different workplaces and tasks.

4. Smart watch ownership was not a mandatory prerequisite for participation, meaning that some participants did not own a smart watch. As a result, they needed to imagine how it would be, and their answers were likely influenced by previous experiences with other devices. However, we have decided to also ask them about their preferences, as we have initially assumed differences with actual users. Such differences could, however, not be observed.

5. Our simulation results are based on the factory settings we have chosen. Since factories differ in size, shape, and other factors, a common factory model to cover all scenarios is almost impossible to establish. As a result, our results cannot be generalized to all factories. They, however, lay the ground for gaining preliminary insights about the feasibility of our presented approach. Besides, the privacy protection offered by spatial cloaking has not been directly measured in our simulations, as our primary focus is to first determine whether and under what conditions the suggested approach is feasible with regards to workers' safety.

8

CONCLUSIONS AND FUTURE WORK

The deployment of smart watches in corporate processes is steadily increasing. Employers are increasingly relying on smart watches as they promise various benefits. These benefits are relevant to both employers and employees. Smart watches promise faster access to information, better employee health, and enhanced workplace safety. However, to achieve their full potential, employees must accept smart watches. However, before smart watches can be introduced into company processes, the employer must involve the works council, if available. The works council can then negotiate a collective agreement with the employer on behalf of the workforce. If there is no works council, this agreement can also be reached by the individual employee for themselves. Nevertheless, before such agreements can be negotiated, employers should be aware of the workforce's willingness and find suitable solutions in advance to inform employees and works council properly about the risks, benefits, and protective measures.

Therefore, in this thesis, we have investigated three different steps in smart watch deployment. We investigated (1) which factors have an influence on the willingness to share data before introducing the smart watch into company processes. These included employees' technological knowledge, legislation knowledge, or technology affinity. (2) We next examined information provided to employees during the introduction of smart watches and how this affects the employees' willingness to share data with employers. (3) Finally, we have proposed privacy-enhancing solutions and studied employees' preferences when smart watches are already deployed for these solutions.

This thesis showed that factors including employees' legislation knowledge, technical affinity, and smart watch ownership influence employees' willingness to share smart watch data with employers. Moreover, we found that employers should not easily expand information about the benefits and risks of smart watches. More information fosters employees' risk awareness, and thus, employees are less likely to share their private information collected with the smart watch. Furthermore, we found that the deployment of privacy-enhancing mechanism spatial cloaking is insufficient considering AGVs' productivity and workplace safety at the same time as bigger cloak radii result in a significant reduction in productivity. In addition, we found that employees would like to disable smart watch data collection, especially in private situations, and would like to be informed about current data collection. In doing so, employees prefer privacy indicators and smart watch interactions, which are more familiar to them.

Based on these findings, we have formulated recommendations for employers for each of the three considered steps to address employees' problems and preferences. Generally speaking, employers are advised to consider employees' wants, needs, and preferences. In addition, employers should never abuse their power to force employees to adopt new technologies.

Although we have explored three stages of smart watch data collection integration in company processes, one step is left. The last step to discover is when employers have already collected smart watch provided data, and employees should be able to access and control such data. Although this step has already received plenty of attention

through privacy dashboards, future research could provide information about smart watch collected data as a report describing which data is used for which purpose. Besides, to evaluate findings under real-world conditions, privacy indicator prototypes and other recommendations we made have to be tested in real-world environments.

REFERENCES

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

[2] C. Anderson and R. Agarwal. "The Digitization of Healthcare: Boundary Risks, Emotion, and Consumer Willingness to Disclose Personal Health Information." In: *Information Systems Research* 22.3 (2011).

[3] S. A. Applin and M. D. Fischer. "Watching Me, Watching You.(Process Surveillance and Agency in the Workplace)." In: *Proc. of the IEEE International Symposium on Technology and Society (ISTAS): Social Implications of Wearable Computing and Augmediated Reality in Everyday Life*. 2013.

[4] L. Ardüser, P. Bissig, P. Brandes, and R. Wattenhofer. "Recognizing Text Using Motion Data From a Smartwatch." In: *IEEE International Conference on Pervasive Computing and Communication Workshops* (2016).

[5] Article 29 Data Protection Working Party. *Opinion 2/2017 on Data Processing at Work (WP249)*. 2017. URL: https://ec.europa.eu/newsroom/article29/items/610169/en.

[6] BMW Group. *Produktionsstart der neuen BMW 7er Limousine*. 2019. URL: https://www.press.bmwgroup.com/austria/article/detail/T0292928DE (visited on 11/31/2021).

[7] N. Backhaus. "Context Sensitive Technologies and Electronic Employee Monitoring: A Meta-Analytic Review." In: *Proc. of the 11th IEEE/SICE international symposium on system integration (SII)*. 2019.

[8] R. Balebako, J. Jung, W. Lu, L. F. Cranor, and C. Nguyen. "'"Little Brothers Watching You" Raising Awareness of Data Leaks on Smartphones." In: *Proc. of the 9th Symposium on Usable Privacy and Security (SOUPS)*. 2013.

[9] L. Bao and S. S. Intille. "Activity Recognition from User-Annotated Acceleration Data." In: *Pervasive Computing*. Ed. by T. Kanade et al. Vol. 3001. Lecture notes in computer science. Springer Berlin Heidelberg, 2004.

[10] J. Barata and P. R. da Cunha. "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)*. 2019.

[11] W. Barfield. *Fundamentals of Wearable Computers and Augmented Reality*. CRC Press, 2015.

[12] D. P. Bhave, L. H. Teo, and R. S. Dalal. "Privacy at Work: A Review and a Research Agenda for a Contested Terrain." In: *Journal of Management* 46.1 (2020).

[13] G. Bieber, T. Kirste, and B. Urban. "Ambient Interaction by Smart Watches." In: *Proc. of the 5th international conference on pervasive technologies related to assistive environments*. 2012.

[14] D. Biswas, I. Aad, and G. P. Perrucci. "Privacy panel: Usable and Quantifiable Mobile Privacy." In: *Proc. of the 8th International Conference on Availability, Reliability and Security (ARES)*. 2013.

[15] M. Boronowsky, O. Herzog, and M. Lawo. "Wearable Computing: Information and Communication Technology Supporting Mobile Workers." In: *it-Information Technology* 50.1 (2008).

[16] CCS Insight. *Healthy Outlook for Wearables As Users Focus on Fitness and Well-Being*. 2021. URL: https://www.ccsinsight.com/press/company-news/healthy-outlook-for-wearables-as-users-focus-on-fitness-and-well-being/ (visited on 05/21/2021).

[17] M. Carley. *Working Time Developments – 2008*. 2009. URL: Online:https://www.eurofound.europa.eu/publications/report/2009/working-time-developments-2008 (visited on 07/12/2019).

[18] D. Carpenter, A. McLeod, C. Hicks, and M. Maasberg. "Privacy and biometrics: An empirical examination of employee concerns." In: *Information Systems Frontiers* 20 (2018).

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

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

[21] B. Choi, S. Hwang, and S. H. Lee. "What Drives Construction Workers' Acceptance of Wearable Technologies in the Workplace?: Indoor Localization and Wearable Health Devices for Occupational Safety and Health." In: *Automation in Construction* 84.1 (2017).

[22] J. Choi and G. O. Ricardo. "Using Heart Rate Monitors to Detect Mental Stress." In: *Proc. of the 6th International Workshop on Wearable and Implantable Body Sensor Networks (BSN)*. 2009.

[23] S. H.-W. Chuah, P. A. Rauschnabel, N. Krey, B. Nguyen, T. Ramayah, and S. Lade. "Wearable Technologies: The Role of Usefulness and Visibility in Smartwatch Adoption." In: *Computers in Human Behavior* 65 (2016).

[24] P. M. Collins and S. Marassi. "Is That Lawful?: Data Privacy and Fitness Trackers in the Workplace." In: *International Journal of Comparative Labour Law* 37.1 (2021).

[25] J. Correa, E. Katz, P. Collins, and M. Griss. *Room-Level Wi-Fi Location Tracking*. Tech. rep. Carnegie Mellon Silicon Valley, 2008.

[26] A. Davoudi, A. A. Wanigatunga, M. Kheirkhahan, D. B. Corbett, T. Mendoza, M. Battula, S. Ranka, R. B. Fillingim, T. M. Manini, and P. Rashidi. "Accuracy of Samsung Gear S Smartwatch for Activity Recognition: Validation Study." In: *JMIR mHealth and uHealth* 7.2 (2019).

[27] K. Degirmenci, J. Shim, M. H. Breitner, F. Nolte, and J. Passlick. "Future of Flexible Work in the Digital Age: Bring Your Own Device Challenges of Privacy Protection." In: *Proc. of the 40th International Conference on Information Systems (ICIS*. 2019.

[28] K. Delac and Grgic M. "A Survey of Biometric Recognition Methods." In: *Proc. of 46th International Symposium Electronics in Marine*. Ed. by T. Kos. Croatian Society Electronics in Marine, 2004.

[29] T. Dinev and P. J. Hart. "An Extended Privacy Calculus Model for E-Commerce Transactions." In: *Information Systems Research* 17.1 (2006).

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

[31] C. Fornell and D. F. Larcker. "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error." In: *Journal of Marketing Research* 18.1 (1981).

[32] D. Gafurov. "A Survey of Biometric Gait Recognition: Approaches, Security and Challenges." In: *Annual Norwegian Computer Science Conference*. 2007.

[33] Gartner Inc. *Gartner Forecasts Global Spending on Wearable Devices to Total $81.5 Billion in 2021*. 2021. URL: https://www.gartner.com/en/newsroom/press-releases/2021-01-11-gartner-forecasts-global-spending-on-wearable-devices-to-total-81-5-billion-in-2021 (visited on 02/14/2021).

[34] D. G. Glance, E. Ooi, Y. Berman, C. F. Glance, and H. R. Barrett. "Impact of a Digital Activity Tracker-Based Workplace Activity Program on Health and Wellbeing." In: *Proc. of the 6th International Conference on Digital Health Conference (DH)*. 2016.

[35] H. Golnabi. "Role of Laser Sensor Systems in Automation and Flexible Manufacturing." In: *Robotics and Computer-Integrated Manufacturing* 19.1-2 (2003).

[36] N. Gorm and I. Shklovski. "Sharing Steps in the Workplace." In: *Proc. of the 34th ACM Conference on Human Factors in Computing Systems (CHI)*. 2016.

[37] A. Grau, M. Indri, L. L. Bello, and T. Sauter. "Industrial Robotics in Factory Automation: From the Early Stage to the Internet of Things." In: *Proc. of the 43rd Annual Conference of the IEEE Industrial Electronics Society (IECON)*. 2017.

[38] J. Han, E. Owusu, L. T. Nguyen, A. Perrig, and J. Zhang. "ACComplice: Location Inference Using Accelerometers on Smartphones." In: *Proc. of the 4th International Conference on Communication Systems and Networks (COMSNETS)*. 2012.

[39] K. Hänsel. "Wearable and Ambient Sensing for Well-Being and Emotional Awareness in the Smart Workplace." In: *Proc. of the ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct (UbiComp)*. 2016.

[40] C. Ilas. "Electronic Sensing Technologies for Autonomous Ground Vehicles: A Review." In: *Proc. of the 8th International Symposium on Advanced Topics in Electrical Engineering (ATEE)*. 2013.

[41] J. Isaak and M. J. Hanna. "User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection." In: *Computer* 51.8 (2018).

[42] J. V. Jacobs, L. J. Hettinger, Y.-H. Huang, S. Jeffries, M. F. Lesch, L. A. Simmons, S. K. Verma, and J. L. Willetts. "Employee Acceptance of Wearable Technology in the Workplace." In: *Applied Ergonomics* 78.1 (2019).

[43] M. Janic, J. P. Wijbenga, and T. Veugen. "Transparency Enhancing Tools (Tets): An Overview." In: *Proc. of the 3rd Workshop on Socio-Technical Aspects in Security and Trust (STAST)*, 2013.

[44] H. Jiang, X. Chen, S. Zhang, X. Zhang, W. Kong, and T. Zhang. "Software for Wearable Devices: Challenges and Opportunities." In: *Proc. of the 39th IEEE Annual Computer Software and Applications Conference Workshops, COMPSACW 2015*. Proceedings - International Computer Software and Applications Conference. 2015.

[45] F. Kehr, T. Kowatsch, D. Wentzel, and E. Fleisch. "Blissfully Ignorant: The Effects of General Privacy Concerns, General Institutional Trust, and Affect in the Privacy Calculus." In: *Information Systems Journal* 25.6 (2015).

[46] Y. Khan, A. E. Ostfeld, C. M. Lochner, A. Pierre, and A. C. Arias. "Monitoring of Vital Signs with Flexible and Wearable Medical Devices." In: *Advanced Materials* 28.22 (2016).

[47] K. Kovacs, F. Ansari, C. Geisert, E. Uhlmann, R. Glawar, and W. Sihn. "A Process Model for Enhancing Digital Assistance in Knowledge-Based Maintenance." In: *Machine Learning for Cyber Physical Systems*. 2019.

[48] M. Kritzler, M. Bäckman, A. Tenfält, and F. Michahelles. "Wearable Technology as a Solution for Workplace Safety." In: *Proc. of the 14th ACM International Conference on Mobile and Ubiquitous Multimedia (MUM)*.

[49] J. Lee Jr, M. Warkentin, R. E. Crossler, and R. F. Otondo. "Implications of Monitoring Mechanisms on Bring Your Own Device Adoption." In: *Journal of Computer Information Systems* 57.4 (2017).

[50] S. W. Lee and K. Mase. "Activity and Location Recognition Using Wearable Sensors." In: *IEEE Pervasive Computing* 1.3 (2002).

[51] M. Lemay, M. Bertschi, J. Sola, P. Renevey, J. Parak, and I. Korhonen. "Application of Optical Heart Rate Monitoring." In: *Wearable sensors*. Elsevier, 2014.

[52] E. Lingg, G. Leone, K. Spaulding, and R. B'Far. "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)*. 2014.

[53] X. Liu, Z. Zhou, W. Diao, Z. Li, and K. Zhang. "When Good Becomes Evil: Keystroke Inference with Smartwatch." In: *Proc. of the of the 22nd ACM Conference on Computer and Communications Security (SIGSAC)*. 2015.

[54] D. Lucke, C. Constantinescu, and E. Westkämper. "Smart Factory-A Step Towards the Next Generation of Manufacturing." In: *Manufacturing Systems and Technologies for the New Frontier*. Springer, 2008.

[55] D. Magni, V. Scuotto, A. Pezzi, and M. Del Giudice. "Employees' Acceptance of Wearable Devices: Towards a Predictive Model." In: *Technological Forecasting and Social Change* 172 (2021).

[56] A. Maiti, M. Jadliwala, J. He, and I. Bilogrevic. "(Smart) Watch Your Taps: Side-Channel Keystroke Inference Attacks Using Smartwatches." In: *Proc. of the ACM International Symposium on Wearable Computers* (2015).

[57] M. Makikawa, N. Shiozawa, and S. Okada. "Fundamentals of Wearable Sensors for the Monitoring of Physical and Physiological Changes in Daily Life." In: *Wearable sensors*. Ed. by E. Sazonov and M. R. Neuman. Academic, 2014.

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

[59] M. Malu and L. Findlater. "Personalized, Wearable Control of a Head-Mounted Display for Users With Upper Body Motor Impairments." In: *Proc. of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. 2015.

[60] A. Manivannan, W. C. B. Chin, A. Barrat, and R. Bouffanais. "On the Challenges and Potential of Using Barometric Sensors to Track Human Activity." In: *Sensors* 20.23 (2020).

[61] S. Mann. "Wearable Computing." In: *Encyclopedia of Human-Computer Interaction* (2012).

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

[63] L. A. McNall and J. M. Stanton. "Private Eyes Are Watching You: Reactions to Location Sensing Technologies." In: *Journal of Business and Psychology* 26 (2011).

[64] R. Meis and M. Heisel. "Understanding the Privacy Goal Intervenability." In: *International Conference on Trust and Privacy in Digital Business*. 2016.

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

[66] T. Mettler and J. Wulf. "Physiolytics at the Workplace: Affordances and Constraints of Wearables Use From an Employee's Perspective." In: *Information Systems Journal* 29.1 (2019).

[67] N. Meyers. "Employee Privacy in the Electronic Workplace: Current Issues for IT Professionals." In: *Proc. of the 14th Australasian Conference on Information Systems (ACIS)*. 2003.

[68] A. Mingkhwan. "WI-FI Tracker: An Organization Wi-Fi Tracking System." In: *Proc. of the 2006 Canadian Conference on Electrical and Computer Engineering*. 2006.

[69] P. V. Moore. *The Quantified Self in Precarity: Work, Technology and What Counts*. 2017.

[70] V. G. Motti and K. Caine. "Users' Privacy Concerns About Wearables." In: *International Conference on Financial Cryptography and Data Security*.

[71] S. C. Mukhopadhyay. "Wearable Sensors for Human Activity Monitoring: A Review." In: *IEEE Sensors Journal* 15.3 (2015).

[72] M. Y. Mun, D. H. Kim, K. Shilton, D. Estrin, M. Hansen, and R. Govindan. "Pdvloc: A Personal Data Vault for Controlled Location Data Sharing." In: *ACM Transactions on Sensor Networks (TOSN)* 10.4 (2014).

[73] P. Murmann and S. Fischer-Hübner. "Tools for Achieving Usable Ex Post Transparency: A Survey." In: *IEEE Access* 5 (2017).

[74] S. Narain, A. Sanatinia, and G. Noubir. "Single-stroke Language-Agnostic Keylogging Using Stereo-Microphones and Domain Specific Machine Learning." In: *Proc. of the 2014 ACM conference on Security and privacy in wireless & mobile networks* (2014).

[75] J. Parkka, M. Ermes, P. Korpipaa, J. Mantyjarvi, J. Peltola, and I. Korhonen. "Activity Classification Using Realistic Data From Wearable Sensors." In: *IEEE Transactions on Information Technology in Biomedicine* 10.1 (2006).

[76] M. Peissner and C. Hipp. *Potenziale der Mensch-Technik-Interaktion für die effiziente und vernetzte Produktion von morgen*. Fraunhofer-Verlag Stuttgart, 2013.

[77] S. Polst, P. Kelbert, and D. Feth. "Company Privacy Dashboards: Employee Needs and Requirements." In: *Proc. of the 1st International Conference on Human-Computer Interaction for Cybersecurity, Privacy and Trust (HCI-CPT)*. 2019.

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

[79] C. Prince. "Do Consumers Want to Control Their Personal Data? Empirical Evidence." In: *International Journal of Human-Computer Studies* 110 (2018).

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

[81] A. Radziwon, A. Bilberg, M. Bogers, and E. S. Madsen. "The Smart Factory: Exploring Adaptive and Flexible Manufacturing Solutions." In: *Procedia engineering* 69 (2014).

[82] N. Ravi, N. Dandekar, P. Mysore, and M. M. L. Littman. "Activity Recognition from Accelerometer Data." In: *Proc. of The 17th Conference on Innovative Applications of Artificial Intelligence* 3 (2005).

[83] R. Rawassizadeh, B. A. Price, and M. Petre. "Wearables: Has the Age of Smartwatches Finally Arrived?" In: *Communications of the ACM* 58.1 (2014).

[84] M. Rodriguez, J. P. Pece, and C. J. Escudero. "In-Building Location Using Bluetooth." In: *International Workshop on Wireless Ad-hoc Networks* (2005).

[85] L. Rook. "Mental models: A robust definition." In: *The learning organization* (2013).

[86] W. Sahqani and L. Turchet. "Co-designing Employees' Data Privacy: a Technology Consultancy Company Use Case." In: *Proc. of the 28th Conference of Open Innovations Association (FRUCT)*. 2021.

[87] A. Sarkisyan, R. Debbiny, and A. Nahapetian. "WristSnoop: Smartphone PINs Prediction Using Smartwatch Motion Sensors." In: *IEEE International Workshop on Information Forensics and Security Proceedings* (2015).

[88] V. Schellewald, B. Weber, R. Ellegast, D. Friemert, and U. Hartmann. "Einsatz von Wearables zur Erfassung der körperlichen Aktivität am Arbeitsplatz." In: *DGUV Forum* 11.1 (2016).

[89] S. Sen, K. K. Rachuri, A. Mukherji, and A. Misra. "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)*. 2016.

[90] W. Shen and G. Newsham. "Smart Phone Based Occupancy Detection in Office Buildings." In: *Proc. of the 20th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*. IEEE, 2016.

[91] M. Shoaib, S. Bosch, H. Scholten, P. J. M. Havinga, and O. D. Incel. "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)*. 2015.

[92] R. Siegel, C. J. König, and V. Lazar. "The Impact of Electronic Monitoring on Employees' Job Satisfaction, Stress, Performance, and Counterproductive Work Behavior: A Meta-Analysis." In: *Computers in Human Behavior Reports* 8 (2022).

[93] P. Siirtola and J. Röning. "Recognizing Human Activities User-independently on Smartphones Based on Accelerometer Data." In: *International Journal of Interactive Multimedia and Artificial Intelligence* 1.5 (2012).

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

[95] A. Stocker, P. Brandl, R. Michalczuk, and M. Rosenberger. "Mensch-zentrierte IKT-Lösungen in einer Smart Factory." In: *e & i Elektrotechnik und Informationstechnik* 131.7 (2014).

[96] E. F. Stone and D. L. Stone. "Privacy in Organizations: Theoretical Issues, Research Findings, and Protection Mechanisms." In: *Research in Personnel and Human Resources Management* 8.3 (1990).

[97] L. Tirabeni. "Technology, Power, and the Organization: Wearable Technologies and Their Implications for the Performance Appraisal." In: *Performance Appraisal in Modern Employment Relations*. 2020.

[98] S. Tisue and U. Wilensky. "NetLogo: A Simple Environment for Modeling Complexity." In: *Proc. of the 7th International Conference on Complex Systems (ICCS)*. 2004.

[99] J. Tolsdorf, F. Dehling, D. Reinhardt, and L. Lo Iacono. "Exploring Mental Models of the Right to Informational Self-Determination of Office Workers in Germany." In: *Proc. on Privacy Enhancing Technologies (PoPETs)* 2021.3 (2021).

[100] J. Tolsdorf, D. Reinhardt, and L. L. Iacono. "Employees' Privacy Perceptions: Exploring the Dimensionality and Antecedents of Personal Data Sensitivity and Willingness to Disclose." In: *Proc. on Privacy Enhancing Technologies (PoPETs)* 2022.2 (2022).

[101] D. L. Tomczak, L. A. Lanzo, and H. Aguinis. "Evidence-based Recommendations for Employee Performance Monitoring." In: *Business Horizons* 61.2 ().

[102] D. L. Tomczak, L. A. Lanzo, and H. Aguinis. "Evidence-based Recommendations for Employee Performance Monitoring." In: *Business Horizons* 61.2 (2018).

[103] S. Trang and W. H. Weiger. "The Perils of Gamification: Does Engaging With Gamified Services Increase Users' Willingness to Disclose Personal Information?" In: *Comput. Hum. Behav.* 116 (2021).

[104] U.S. Bureau of Labor Statistics. *Average Weekly Hours of All Employees: Manufacturing [AWHAEMAN]*. 2019. URL: Online:https://fred.stlouisfed.org/series/AWHAEMAN (visited on 07/12/2019).

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

[106] H. Wang, T. T.-T. Lai, and R. Roy Choudhury. "MoLe: Motion Leaks through Smartwatch Sensors." In: *Proc. of the 21st Annual International Conference on Mobile Computing and Networking*. ACM, 2015.

[107] D. L. Wells, R. H. Moorman, and J. M. Werner. "The Impact of the Perceived Purpose of Electronic Performance Monitoring on an Array of Attitudinal Variables." In: *Human Resource Development Quarterly* 18.1 (2007).

[108] A. F. Westin. *Privacy and Freedom*. Atheneum, 1967.

[109] U. Wilensky, E. Hazzard, and R. Froemke. "GasLab: An Extensible Modeling Toolkit for Exploring Statistical Mechanics." In: *Proc. of the 7th European Logo Conference (EUROLOGO)*. 1999.

[110] J. Winkley, P. Jiang, and W. Jiang. "Verity: An Ambient Assisted Living Platform." In: *IEEE Transactions on Consumer Electronics* 58.2 (2012).

[111] M. Wu, P. H. Pathak, and P. Mohapatra. "Monitoring Building Door Events U sing Barometer Sensor in Smartphones." In: *Proc. of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing*. Ed. by K. Mase, M. Langheinrich, D. Gatica-Perez, H. Gellersen, T. Choudhury, and K. Yatani. ACM, 2015.

[112] J.-S. Yoon, S.-J. Shin, and S.-H. Suh. "A Conceptual Framework for the Ubiquitous Factory." In: *International Journal of Production Research* 50.8 (2012).

[113] Zebra Technologies. *Quality Drives a Smarter Plant Floor: Manufacturing Vision Study*. 2017. URL: https://www.zebra.com/content/dam/zebra_new_ia/en-us/solutions-verticals/vertical-solutions/manufacturing/white-papers/2017-manufacturing-vision-study-en-emea.pdf (visited on 09/21/2021).

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

[115] X. Zhang, S. Liu, X. Chen, L. Wang, B. Gao, and Q. Zhu. "Health Information Privacy Concerns, Antecedents, and Information Disclosure Intention in Online Health Communities." In: *Information & Management* 55.4 (2018).

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