Exploration of Factors that Can Impact the Willingness of Employees to Share Smart Watch Data with Their Employers

Alexander Richter, Patrick Kühtreiber, Delphine Reinhardt

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

Alexander Richter[1], Patrick Kühtreiber[1], and Delphine Reinhardt[1,2]

[1] Computer Security and Privacy, University of Göttingen
Goldschmidtstr. 7, 37073 Göttingen, Germany
[2] Campus Institute Data Science
Goldschmidtstr. 1, 37073 Göttingen, Germany
richter@cs.uni-goettingen.de, kuehtreiber@cs.uni-goettingen.de,
reinhardt@cs.uni-goettingen.de

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

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. 2. We introduce our research goals in Sec. 3 and applied methodology in Sec. 4. We present our results in Sec. 5 with a focus on our hypotheses and discuss our results in Sec. 6. We further discuss our findings and recommendations in Sec. 7, before making concluding remarks in Sec. 8.

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 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.

4 Methodology

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. 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.

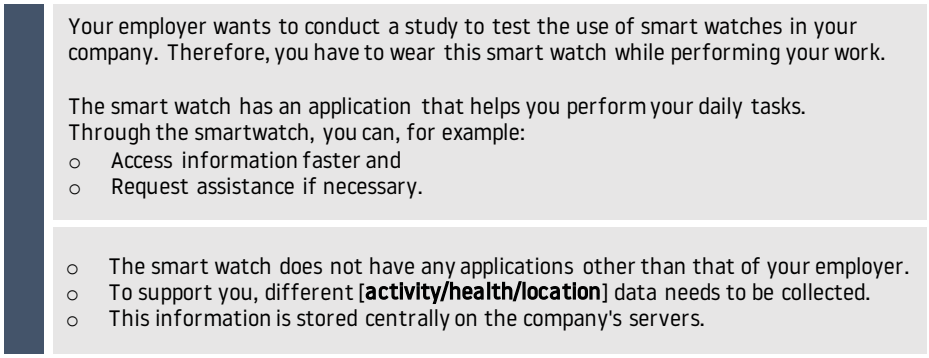

Fig. 1. Provided scenario

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 Tab. 3 in Appendix A).

Next, we have asked the participants whether they own a smart watch and to respectively provide information about their usage (see Tab. 4 in Appendix A). Besides, we have asked them different questions about (1) smart watches' capability regarding data collection and processing (see Tab. 5 in Appendix A) and (2) legislation frameworks (see Tab. 6 and 7 in Appendix A) in order to quantify their knowledge and understanding about both matters. We have finally evaluated their technical affinity using questions from [10] (see Tab. 8 in Appendix A).

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.

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.

5 Results

In this section, we detail the obtained results, while we specifically test our hypotheses formulated in Sec. 6.

5.1 Demographics

As shown in Tab. 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 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%).

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 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 ($p = 0.005$).

Table 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%

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 Tab. 5), and that these data can be used to draw inferences about their health (70.1%, Q_{TK2} in Tab. 5). In addition, a majority of the participants (61.6%, Q_{TK3} in Tab. 5) 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. 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.

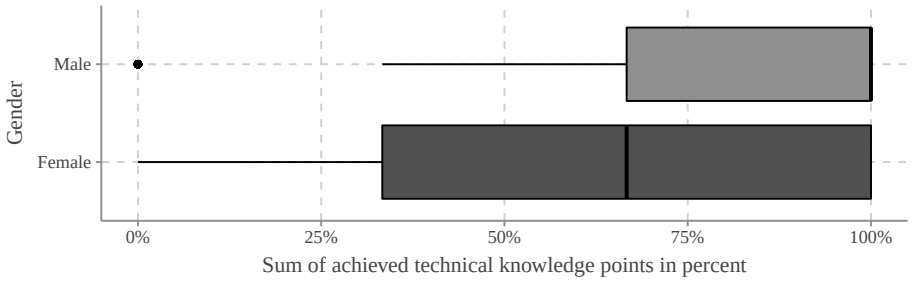

Fig. 2. Participants' technical knowledge score about smart watch capabilities per gender

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 General Data Protection Regulation (GDPR) purpose (23.8%) or have incorrect knowledge about it (31.8%, Q_{LK1} in Tab. 6). 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 Tab. 6). Positively, the majority know when the processing of personal data is lawful (61.8%, Q_{LK3} in Tab. 6) or whereby consent to the collection of personal data occurs (60.7%, Q_{LK4} in Tab. 6). However, some respondents stated that they do not know (17.9%, Q_{LK3}/22.1%, Q_{LK4} in Tab. 6). 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 Tab. 7).

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

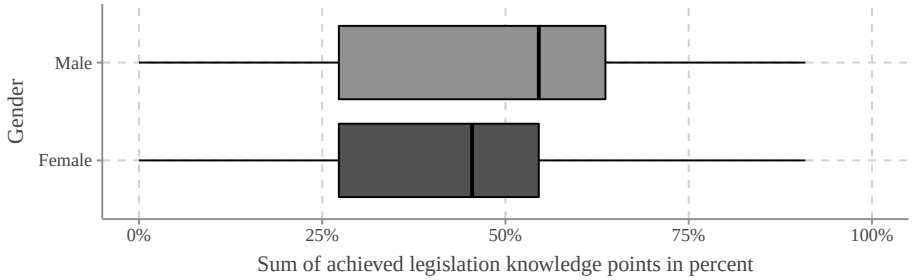

Fig. 3. Participants' legislation knowledge score per gender

of agreement to collect and use employees' data (Q_{LK6} in Tab. 7). 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 Tab. 7). 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 Tab. 7). 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 Tab. 7). 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 Tab. 7) 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 Tab. 7). When looking at the aggregated results over the 11 questions (each correct answer corresponding to one point), an average 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. Fig. 4 shows differences in achieved legislation knowledge points between the specified functions, while Fig. 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 knowl-

edge ($p = 0.006$, 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.

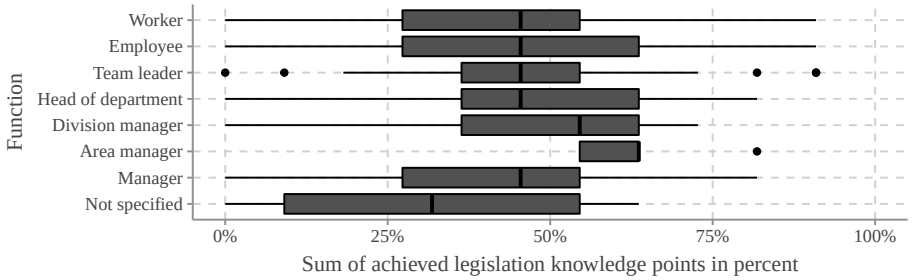

Fig. 4. Participants' legislation knowledge score per function

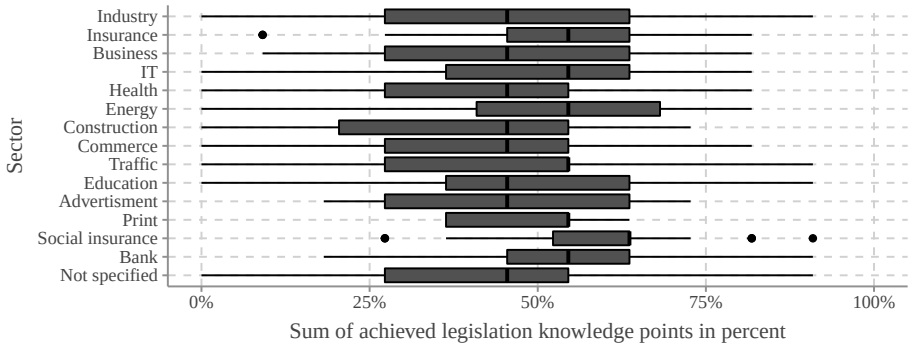

Fig. 5. Participants' legislation knowledge score per sector

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 ($p = 0.001$).

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 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.

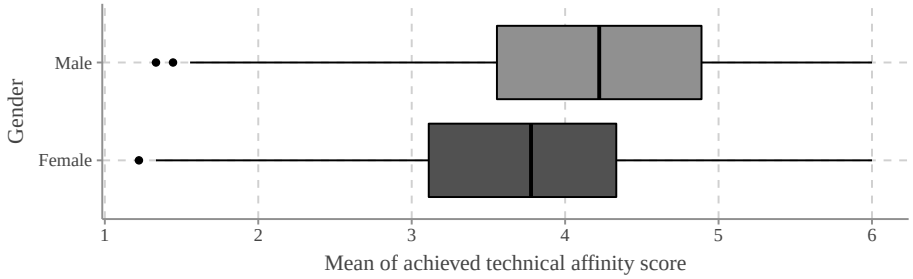

Fig. 6. Participants' technical affinity score per gender

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 Tab. 3 in Appendix 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.

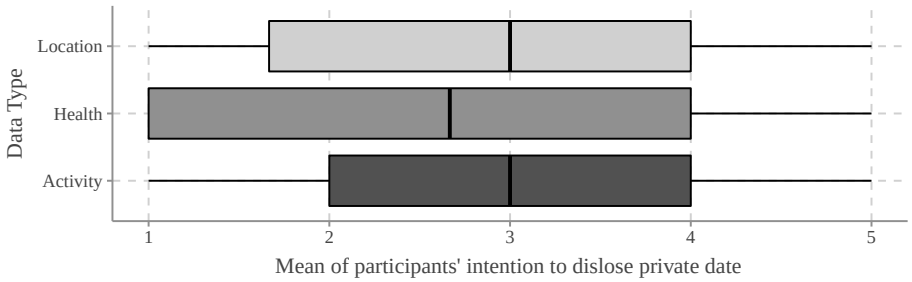

Fig. 7. Means of participants' intention to disclose for each data type

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 Tab. 3) 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. Fig. 7 presents and Tab. 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 2. Data type mean overview

Type	N	M	SD	MIN	MAX	$\Delta Activity$	$\Delta Health$
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		

6 Testing the hypotheses

In the following, we test our hypotheses defined in Section 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 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 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 $Q_{TK1} - Q_{TK3}$ (Tab. 5 in Appendix 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 employ-

ees' willingness to disclose data to their employers. Consequently, H2 is not supported.

However, to sum up, considering our findings in Section 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 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 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.

7 Discussion

Derived from our results presented in Sections 5 and 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.

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.

9 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. Applin, S.A., Fischer, M.D.: 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. pp. 268–275 (2013)
2. BMW Group: Produktionsstart der neuen BMW 7er Limousine (2019), https://www.press.bmwgroup.com/austria/article/detail/T0292928DE
3. CCS Insight: Healthy Outlook for Wearables As Users Focus on Fitness and Well-Being (2021), https://www.ccsinsight.com/press/company-news/healthy-outlook-for-wearables-as-users-focus-on-fitness-and-well-being/
4. Choi, B., Hwang, S., Lee, S.H.: What Drives Construction Workers' Acceptance of Wearable Technologies in the Workplace?: Indoor Localization and Wearable Health Devices for Occupational Safety and Health. Automation in Construction **84**(1), 31–41 (2017)
5. Cohen, J.: Statistical Power Analysis for the Behavioral Sciences. Academic press (1988)
6. Collins, P.M., Marassi, S.: Is That Lawful?: Data Privacy and Fitness Trackers in the Workplace. International Journal of Comparative Labour Law **37**(1), 65–94 (2021)
7. Datta, P., Namin, A.S., Chatterjee, M.: A Survey of Privacy Concerns in Wearable Devices. In: Proc. of the IEEE International Conference on Big Data (Big Data). pp. 4549–4553 (2018)
8. Davoudi, A., Wanigatunga, A.A., Kheirkhahan, M., Corbett, D.B., Mendoza, T., Battula, M., Ranka, S., Fillingim, R.B., Manini, T.M., Rashidi, P.: Accuracy of Samsung Gear S Smartwatch for Activity Recognition: Validation Study. JMIR mHealth and uHealth **7**(2), e11270 (2019)
9. Dinev, T., Hart, P.J.: An extended privacy calculus model for e-commerce transactions. Information Systems Research **17**(1), 61–80 (2006)
10. Franke, T., Attig, C., Wessel, D.: A Personal Resource for Technology Interaction: Development and Validation of the Affinity for Technology Interaction (Ati) Scale. International Journal of Human–Computer Interaction **35**(6), 456–467 (2019)
11. Gorm, N., Shklovski, I.: Sharing Steps in the Workplace. In: Proc. of the 34th ACM Conference on Human Factors in Computing Systems (CHI). pp. 4315–4319 (2016)
12. Isaak, J., Hanna, M.J.: User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. Computer **51**(8), 56–59 (2018)
13. Jacobs, J.V., Hettinger, L.J., Huang, Y.H., Jeffries, S., Lesch, M.F., Simmons, L.A., Verma, S.K., Willetts, J.L.: Employee Acceptance of Wearable Technology in the Workplace. Applied Ergonomics **78**(1), 148–156 (2019)
14. Kehr, F., Kowatsch, T., Wentzel, D., Fleisch, E.: Blissfully Ignorant: The Effects of General Privacy Concerns, General Institutional Trust, and Affect in the Privacy Calculus. Information Systems Journal **25**(6), 607–635 (2015)

15. Kline, R.B.: Principles and practice of structural equation modeling. Methodology in the social sciences, New York, fourth edition edn. (2016)
16. Kovacs, K., Ansari, F., Geisert, C., Uhlmann, E., Glawar, R., Sihn, W.: A Process Model for Enhancing Digital Assistance in Knowledge-Based Maintenance. In: Machine Learning for Cyber Physical Systems, pp. 87–96 (2019)
17. Kritzler, M., Bäckman, M., Tenfält, A., Michahelles, F.: Wearable Technology as a Solution for Workplace Safety. In: Proc. of the 14th ACM International Conference on Mobile and Ubiquitous Multimedia (MUM). pp. 213–217. ACM (2015)
18. Mekruksavanich, S., Hnoohom, N., Jitpattanakul, A.: Smartwatch-Based Sitting Detection With Human Activity Recognition for Office Workers Syndrome. In: 2018 IEEE International ECTI Northern Section Conference on Electrical, Electronics, Computer and Telecommunications Engineering (ECTI-NCON). pp. 160–164 (2018)
19. Moore, P.V.: The Quantified Self in Precarity: Work, Technology and What Counts (2017)
20. Motti, V.G., Caine, K.: Users' Privacy Concerns About Wearables. In: International Conference on Financial Cryptography and Data Security. pp. 231–244 (2015)
21. Ozdemir, Z.D., Smith, H.J., Benamati, J.H.: Antecedents and Outcomes of Information Privacy Concerns in a Peer Context: An Exploratory Study. European Journal of Information Systems **26**(6), 642–660 (2017)
22. Prince, C.: Do Consumers Want to Control Their Personal Data? Empirical Evidence. International Journal of Human-Computer Studies **110**, 21–32 (2018)
23. Prince, C., Omrani, N., Maalaoui, A., Dabic, M., Kraus, S.: Are We Living in Surveillance Societies and Is Privacy an Illusion? An Empirical Study on Privacy Literacy and Privacy Concerns. IEEE Transactions on Engineering Management (2021)
24. Schaub, F., Marella, A., Kalvani, P., Ur, B., Pan, C., Forney, E., Cranor, L.F.: Watching Them Watching Me: Browser Extensions' Impact on User Privacy Awareness and Concern. In: Proc. of the 2016 Workshop on Usable Security (USEC). pp. 1–10 (2016)
25. Schellewald, V., Weber, B., Ellegast, R., Friemert, D., Hartmann, U.: Einsatz von Wearables zur Erfassung der körperlichen Aktivität am Arbeitsplatz. DGUV Forum **11**(1), 36–37 (2016)
26. Shoaib, M., Bosch, S., Scholten, H., Havinga, P.J., Incel, O.D.: 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). pp. 591–596 (2015)
27. Statista Inc.: Do you personally use wearables (e.g. smart watch, health / fitness tracker)? [Graph] (2021), https://www.statista.com/forecasts/1101110/wearables-devices-usage-in-selected-countries
28. Statistisches Bundesamt (Destatis): 12111-0004: Bevölkerung (Zensus): Deutschland, Stichtag, Geschlecht, Altersgruppen (2021), https://www-genesis.destatis.de/genesis/online
29. Stocker, A., Brandl, P., Michalczuk, R., Rosenberger, M.: Mensch-zentrierte IKT-Lösungen in einer Smart Factory. e & i Elektrotechnik und Informationstechnik **131**(7), 207–211 (2014)
30. Sun, Y., Wang, N., X., S.: Perceived Benefits, Privacy Risks, and Perceived Justice in Location Information Disclosure: a Moderated Mediation Analysis. In: Proc. of the 2014 Pacific Asia Conference on Information Systems (PACIS) (2014)

31. Tomczak, D.L., Lanzo, L.A., Aguinis, H.: Evidence-based Recommendations for Employee Performance Monitoring. Business Horizons **61**(2), 251–259 (2018)
32. Trang, S., Weiger, W.H.: The Perils of Gamification: Does Engaging With Gamified Services Increase Users' Willingness to Disclose Personal Information? Comput. Hum. Behav. **116**, 106644 (2021)
33. Wang, T., Duong, T.D., Chen, C.C.: Intention to Disclose Personal Information via Mobile Applications: A Privacy Calculus Perspective. International Journal of Information Management **36**(4), 531–542 (2016)
34. Wirtz, J., Lwin, M.O., Williams, J.D.: Causes and consequences of consumer online privacy concern. International Journal of Service Industry Management **18**(4), 326–348 (2007)
35. Xu, H., Teo, H.H., Tan, B.C., Agarwal, R.: The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services. Journal of management information systems **26**(3), 135–174 (2009)
36. Zhang, X., Liu, S., Chen, X., Wang, L., Gao, B., Zhu, Q.: Health Information Privacy Concerns, Antecedents, and Information Disclosure Intention in Online Health Communities. Information & Management **55**(4), 482–493 (2018)
37. Ziegler, J., Heinze, S., Urbas, L.: The Potential of Smartwatches to Support Mobile Industrial Maintenance Tasks. In: Proc. of the 20th IEEE Conference on Emerging Technologies Factory Automation (ETFA). pp. 1–7 (2015)

A Questions

Table 3. 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 4. 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 5. 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 6. 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 7. 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 8. 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*