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

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
lastname@cs.uni-goettingen.de

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

1 Introduction

More and more smart watches are sold worldwide [15, 19]. In addition to be used for private purposes, companies also recognize their potential and increasingly equip their employees with such devices [21, 42]. For example, they are used for allowing faster access to information [28, 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

* The final publication is available at Springer via http://dx.doi.org/10.1007/978-3-031-06975-8_3

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 General Data Protection Regulation (GDPR), especially in Art. 5 (1) and Recitals 58 and 60. Although previous research on transparency mechanisms to increase privacy awareness exists [17, 8, 3, 1], 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 [9, 20, 24, 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. 1) and considered six different control interactions (see Fig. 2), 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. 1(a)) 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. 2, we review related work. We present our research goals in Sec. 3. We detail our decision drivers in Sec. 4 and 5. We present our methodology in Sec. 6 and our results in Sec. 7, which we discuss in Sec. 8, and make concluding remarks in Sec. 9.

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 [32], 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 [32]. 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 [32]. However, in the context of smart watches, privacy concerns can arise in many ways [12, 27], 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 [6, 12, 34]. As a result, this can negatively impact workers' job satisfaction and stress levels, leading to productivity declines [23, 38].

In the second category, previous studies are dedicated to raising privacy awareness by nudging through visual indicators [17], warning messages [8, 3, 1, 35] 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 [8] 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 [35]. 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 [7]. For example, smart speakers provide mute buttons to stop the microphone functions [20, 24]. 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 [9] 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.

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 [33]. Such indicators may be textual, graphic, or audible [33]. Meanwhile, many IoT devices including smart speakers [10, 18, 20] are equipped with an LED that indicates data collection [31]. 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?

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.

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 [26, 29, 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.

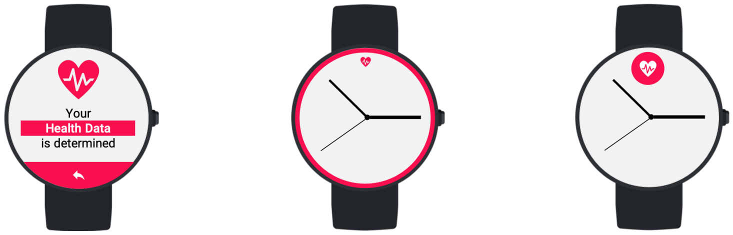
Secondly, smart watches are constrained by size and shape. Compared to smartphones, their screen is even smaller. Since smart watch wearers only briefly check the screen [30], the provided information should be as brief as possible to accommodate the screen size and not to appear cluttered, while providing 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.

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.

Design A: Splash-screen The first design shown in Fig. 1(a) is the most common and known as a notification. It is motivated by [17, 35] and represents a normal notification, which the wearer must actively close. The used color depends on the



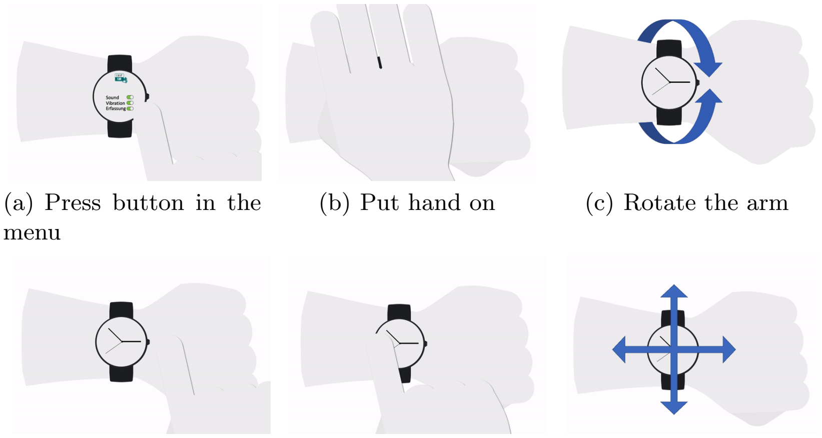
(a) Splash-screen design (b) Circular design (c) Icon design

Fig. 1. Examples of proposed indicators to visualize the collection of health data on a smart watch

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. 1(b) 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. 1(c) 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.



(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

Fig. 2. Proposed mechanisms to interrupt personal data collection on a smart watch

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).

5.1 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.

5.2 Selected Control Interactions

In the following, we describe the selected control interactions illustrated in Fig. 2, which enable the user to interrupt the data collection.

Interaction A: Press a button in the menu Fig. 2(a) 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. 2(b) 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. 2(c) 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. 2(d) 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. 2(e) 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. 2(f) shows our second real gesture. Similar to the gesture in Fig. 2(c), 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.

6 Methodology

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 [13]. In total, 1,033 participants answered our questionnaire in August 2021.

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. 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. 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. 2). 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).

7 Results

7.1 Demographics

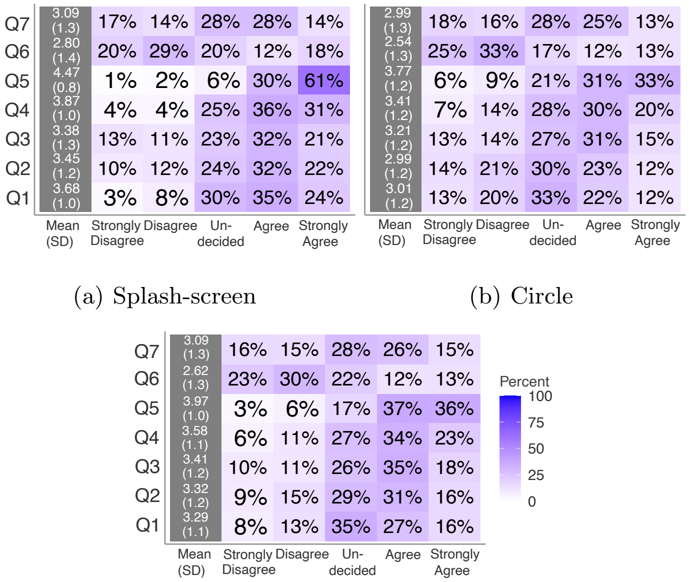
Among our 1,033 participants, 48% are women and 52% are men. Their age distribution matches the current population of Germany [13]. A majority of our participants work in health and social care (15%) followed by industry (14%), public service (7%), and IT/telecom (6%). Their working conditions are as 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.

7.2 Preferences for Privacy Indicators

When considering our three privacy indicators (see Fig. 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. 3) 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 [11]. In all sub-questions, except sub-question three, the splash-screen design reaches higher means, shown in Fig. 3. 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.

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 [22] 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.

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 ($\chi^2_{(1)} = 15.67, p < .001$).



(a) Splash-screen

(b) Circle

(c) Icon

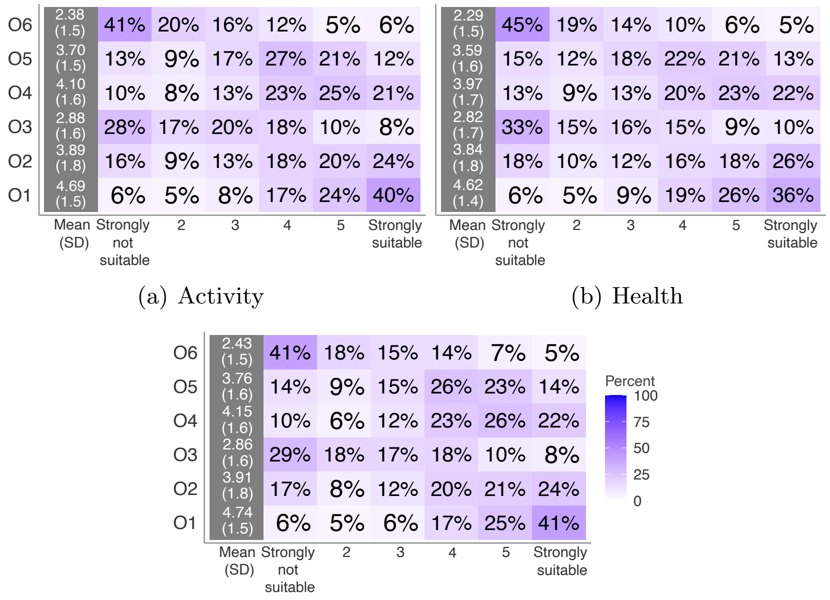
Fig. 3. Results of proposed privacy indicators. Attitude on "This privacy indicator... (Q1) would reinforce my perception about data collection. (Q2) would catch my general attention. (Q3) seems to me to be useful for the purpose. (Q4) is intuitive. (Q5) is easy to understand. (Q6) is disturbing. (Q7) is acceptable in order to visualize the data collection."

7.3 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. 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. 4 show the results for each 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.

Table 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

	Mean (SD)	Strongly not suitable	2	3	4	5	Strongly suitable
O6	2.38 (1.5)	41%	20%	16%	12%	5%	6%
O5	3.70 (1.5)	13%	9%	17%	27%	21%	12%
O4	4.10 (1.6)	10%	8%	13%	23%	25%	21%
O3	2.88 (1.6)	28%	17%	20%	18%	10%	8%
O2	3.89 (1.8)	16%	9%	13%	18%	20%	24%
O1	4.69 (1.5)	6%	5%	8%	17%	24%	40%

(b) Health

	Mean (SD)	Strongly not suitable	2	3	4	5	Strongly suitable
O6	2.29 (1.5)	45%	19%	14%	10%	6%	5%
O5	3.59 (1.6)	15%	12%	18%	22%	21%	13%
O4	3.97 (1.7)	13%	9%	13%	20%	23%	22%
O3	2.82 (1.7)	33%	15%	16%	15%	9%	10%
O2	3.84 (1.8)	18%	10%	12%	16%	18%	26%
O1	4.62 (1.4)	6%	5%	9%	19%	26%	36%

(c) Location

	Mean (SD)	Strongly not suitable	2	3	4	5	Strongly suitable
O6	2.43 (1.5)	41%	18%	15%	14%	7%	5%
O5	3.76 (1.6)	14%	9%	15%	26%	23%	14%
O4	4.15 (1.6)	10%	6%	12%	23%	26%	22%
O3	2.86 (1.6)	29%	18%	17%	18%	10%	8%
O2	3.91 (1.8)	17%	8%	12%	20%	21%	24%
O1	4.74 (1.5)	6%	5%	6%	17%	25%	41%

Fig. 4. 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

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.

8.1 Privacy Indicators

Our first research question (see Sec. 3) focuses on analyzing which privacy indicators are perceived by employees as sufficient and useful to visualize data collection. The results described in Sec. 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.

Additional Feedback. In addition to the visual elements of such indicators, the results shown in Sec. 7 indicate that participants' opinions differ regarding supplementary feedback, either a sound or vibrations. Thus, the findings from [25] 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 [29] and that such notifications are disruptive on smartphones [26, 29]. A reduction of those interruptions could be possible in a professional context by deferring notification [29], especially when it comes to privacy notifications, as users usually consider standard app notifications to be more important than privacy notifications [25]. Therefore, less noticeable notifications such as silent mode should be possible [25] because even then, privacy notifications would be read according to [25]. 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.

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.

8.2 Control Interactions

Overall, our results presented in Sec. 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. 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).

8.3 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 smartwatch 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.

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. 1(a)) to visualize data collection followed by the icon (Fig. 1(c)) and the circle indicator (Fig. 1(b)). 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. Almuhimedi, H., Schaub, F., Sadeh, N., Adjerid, I., Acquisti, A., Gluck, J., Cranor, L.F., Agarwal, Y.: 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), https://support.apple.com/en-us/HT211876, (accessed: 2021-09-09)
3. Bal, G., Rannenberg, K., Hong, J.: 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. Barata, J., da Cunha, P.R.: 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. Bovard, P.P., Sprehn, K.A., Cunha, M.G., Chun, J., Kim, S., Schwartz, J.L., Garver, S.K., Dey, A.K.: Multi-Modal Interruptions on Primary Task Performance. In: Proc. of the 12th International Conference on Augmented Cognition (AC) (2018)
6. 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) (2017)
7. Christin, D., Engelmann, F., Hollick, M.: Usable Privacy for Mobile Sensing Applications. In: Proc. of the 8th Workshop on Information Security Theory and Practice (WISTP). vol. 8501 (2014)

8. Christin, D., Michalak, M., Hollick, M.: 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)
9. Christin, D., Reinhardt, A., Hollick, M., Trumpold, K.: Exploring User Preferences for Privacy Interfaces in Mobile Sensing Applications. In: Proc. of 11th ACM International Conference on Mobile and Ubiquitous Multimedia (MUM) (2012)
10. Chung, H., Iorga, M., Voas, J.M., Lee, S.: ”Alexa, Can I Trust You?”. Computer **50**(9) (2017)
11. Cortina, J.M.: What Is Coefficient Alpha? An Examination of Theory and Applications. Journal of applied psychology **78**(1) (1993)
12. Datta, P., Namin, A.S., Chatterjee, M.: A Survey of Privacy Concerns in Wearable Devices. In: Proc. of the 2018 IEEE International Conference on Big Data (Big Data) (2018)
13. (Destatis), S.B.: 12111-0004: Bevölkerung (Zensus): Deutschland, Stichtag, Geschlecht, Altersgruppen (2021), https://www-genesis.destatis.de/genesis/online
14. 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) (2019)
15. Gartner Inc.: Gartner Forecasts Global Spending on Wearable Devices to Total $81.5 Billion in 2021 (2021), 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, (accessed: 2021-02-14)
16. Glance, D.G., Ooi, E., Berman, Y., Glance, C.F., Barrett, H.R.: 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. Hassib, M., Abdelmoteleb, H., Khamis, M.: 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. Hernández Acosta, L., Reinhardt, D.: A Survey on Privacy Issues and Solutions for Voice-Controlled Digital Assistants. Pervasive and Mobile Computing (2021)
19. Insight, C.: 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/, (accessed: 2021-09-21)
20. Lau, J., Zimmerman, B., Schaub, F.: Alexa, Are You Listening?: Privacy Perceptions, Concerns and Privacy-seeking Behaviors with Smart Speakers. ACM Human-Computer Interactions **2**(CSCW) (2018)
21. Maltseva, K.: Wearables in the Workplace: The Brave New World of Employee Engagement. Business Horizons (2020)
22. Mayring, P.: Qualitative Content Analysis. A companion to qualitative research **1**(2) (2004)
23. Meyers, N.: Employee Privacy in the Electronic Workplace: Current Issues for IT Professionals. In: Proc. of the 14th Australasian Conference on Information Systems (ACIS) (2003)
24. Mhaidli, A.H., Venkatesh, M.K., Zou, Y., Schaub, F.: Listen Only When Spoken To: Interpersonal Communication Cues as Smart Speaker Privacy Controls. In: Proc. of the 20st Privacy Enhancing Technologies Symposium (PoPETs) (2020)

25. Micallef, N., Just, M., Baillie, L., Alharby, M.: 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)
26. Mirzamohammadi, S., Sani, A.A.: Viola: Trustworthy Sensor Notifications for Enhanced Privacy on Mobile Systems. IEEE Transactions on Mobile Computing **17**(11) (2018)
27. Motti, V.G., Caine, K.: Users' Privacy Concerns About Wearables. In: Proc. of the 18th International Conference on Financial Cryptography and Data Security (FC). Springer (2015)
28. Peissner, M., Hipp, C.: Potenziale der Mensch-Technik-Interaktion für die effiziente und vernetzte Produktion von morgen. Fraunhofer-Verlag Stuttgart (2013)
29. Pielot, M., Church, K., de Oliveira, R.: 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)
30. Pizza, S., Brown, B., McMillan, D., Lampinen, A.: Smartwatch in Vivo. In: Proc. of the 34th Conference on Human Factors in Computing Systems (CHI) (2016)
31. Prange, S., Shams, A., Piening, R., Abdelrahman, Y., Alt, F.: PriView- Exploring Visualisations to Support Users' Privacy Awareness. In: Proc. of the ACM Conference on Human Factors in Computing Systems (CHI) (2021)
32. Raij, A., Ghosh, A., Kumar, S., Srivastava, M.: 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)
33. Reidenberg, J.R., Russell, N.C., Herta, V., Sierra-Rocafort, W., Norton, T.B.: Trustworthy Privacy Indicators: Grades, Labels, Certifications, and Dashboards. Wash. UL Rev. **96** (2018)
34. Schall, M.C.J., Sesek, R.F., Cavuoto, L.A.: Barriers to the Adoption of Wearable Sensors in the Workplace: A Survey of Occupational Safety and Health Professionals. Human Factors **60**(3) (2018)
35. Shaw, P.A., Mikusz, M.A., Davies, N.A.J., Clinch, S.E.: Using Smartwatches for Privacy Awareness in Pervasive Environments. Poster at the 18th International Workshop on Mobile Computing Systems and Applications (HotMobile) (2017)
36. Stocker, A., Brandl, P., Michalczuk, R., Rosenberger, M.: Mensch-zentrierte IKT-Lösungen in einer Smart Factory. e & i Elektrotechnik und Informationstechnik **131**(7) (2014)
37. Tiefenau, C., Häring, M., Gerlitz, E., von Zezschwitz, E.: Making Privacy Graspable: Can we Nudge Users to use Privacy Enhancing Techniques? CoRR (2019)
38. Tomczak, D.L., Lanzo, L.A., Aguinis, H.: Evidence-Based Recommendations for Employee Performance Monitoring. Business Horizons **61**(2) (2018)
39. Udoh, E.S., Alkharashi, A.: 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. Weber, D., Voit, A., Le, H.V., Henze, N.: 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. Williams, M., Nurse, J.R., Creese, S.: (Smart) Watch Out! Encouraging Privacy-Protective Behavior Through Interactive Games. International Journal of Human-Computer Studies **132** (2019)
42. Zebra Technologies: Quality Drives a Smarter Plant Floor: Manufacturing Vision Study (2017)