Taylor & Francis
Taylor & Francis Group

Production & Manufacturing Research

An Open Access Journal

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/tpmr20

Location-based monitoring in production environments: does transparency help to increase the acceptance of monitoring?

Christian Jandl, Setareh Zafari, Florian Taurer, Martina Hartner-Tiefenthaler & Sebastian Schlund

To cite this article: Christian Jandl, Setareh Zafari, Florian Taurer, Martina Hartner-Tiefenthaler & Sebastian Schlund (2023) Location-based monitoring in production environments: does transparency help to increase the acceptance of monitoring?, Production & Manufacturing Research, 11:1, 2160387, DOI: 10.1080/21693277.2022.2160387

To link to this article: https://doi.org/10.1080/21693277.2022.2160387

Published online: 03 Jan 2023.

PRODUCTION & MANUFACTURING RESEARCH
2023, VOL. 11, NO. 1, 2160387
https://doi.org/10.1080/21693277.2022.2160387

Taylor & Francis
Taylor & Francis Group

ARTICLE

OPEN ACCESS Check for updates

Location-based monitoring in production environments: does transparency help to increase the acceptance of monitoring?

Christian Jandl[a*], Setareh Zafari[b*], Florian Taurer[a], Martina Hartner-Tiefenthaler[b] and Sebastian Schlund[b]

[a]Department Media Technologies, Institute of Creative\Media/Technologies, St. Pölten, Austria; [b]Faculty of Mechanical and Indusrial Engineering, Institute of Management Science, TU Wien, Wien, Austria

ABSTRACT

In the context of smart manufacturing, the technical development of monitoring systems has made it possible to track employees with the same systems that are used to track assets. This study contributes to our understanding of the acceptance of location-based monitoring of employees and investigates how the perceived privacy risk regarding monitoring can be tackled by examining the role of transparency and the perceived value of monitoring. We designed an experimental setting in which students assembled a 3D printer and manipulated transparency with two conditions: a detailed explanation of monitoring during the task vs. monitoring without any explanation. The results show that the higher the privacy concerns and perceived risks were, the lower was the acceptance for monitoring. However, the negative effect of perceived risk diminishes when both, transparency and the value of monitoring are high, but becomes even stronger when only transparency is high and perceived value is low.

ARTICLE HISTORY
Received 5 October 2022
Accepted 14 December 2022

KEYWORDS
Privacy; employee location monitoring; tracking and tracing; transparency

1. Introduction

Employee monitoring (EM) and its impact on the working environment is a widely discussed topic in the field of organizational research. People engaged in employee monitoring often have strongly differing views on economic, ethical, and legal issues (Kaupins & Minch, 2005). A more comprehensive inquiry into ethical concerns is necessary to understand the complexity of EM (Martin & Freeman, 2002). On the one hand, it is argued that EM may improve work performance, security and safety (Bhave, 2013; Lucas et al., 2016), while on the other hand, EM raises questions regarding engagement, privacy and social control of employees (McNall & Roch, 2007; Zweig & Webster, 2003).

Nowadays, companies can precisely record and automatically analyse extensive amounts of data. The development of monitoring systems in the context of smart manufacturing has made it technically feasible to track and trace employees using the same systems that are normally used to track assets. In the context of smart

CONTACT Christian Jandl cjandl@fhstp.ac.at Christian Jandl, Campus Platz 1, St. Pölten, 3100, Austria
*These authors contributed equally to this project and should be considered co-first authors.

manufacturing, people can also be seen as 'things' to be monitored and connected with each other or with machines.

Employee location monitoring (ELM) refers to emerging technologies that enable an organization to monitor and determine the location of its employees in near real time outdoors with the Global Navigation Satellite System or inside buildings with wireless sensor networks (Kaupins & Minch, 2005). Thus, modern tracking and tracing systems offer a broad range of functionality to monitor employees, who may not be aware of this tracking. Although EM has advantages for organizations and potentially also for employees themselves, like a safer workplace where working conditions are hazardous (e.g. tunneling, mining or a better overview of a construction site, Jandl et al., 2021), the extent to which employees feel that monitoring is an invasion of privacy will likely influence their acceptance of monitoring (Abraham et al., 2019; Alder, 2001). Furthermore, EM might enable supervisors to obtain more information about their subordinates' behavior, which could lead to a feeling of permanent surveillance and pressure to perform, resulting in stress and strain without any beneficial effects on performance (Ravid et al., 2022). This might be particularly relevant when employees do not know what data is being collected and for what purposes monitoring is taking place. Previous studies have found that increasing transparency regarding the types and purposes of data collection can minimize people's negative attitudes (Anderson & Agarwal, 2011; McNall & Roch, 2007; ten Berg et al., 2019). Therefore, it is necessary to thoroughly weigh the effects of transparency and understand when transparency positively influences employees' acceptance of being monitored.While some research has been carried out on the impact of location monitoring procedures on employees' attitudes and acceptance (Jeske & Santuzzi, 2015; Jeske, 2022; Wells et al., 2007), there have been few empirical investigations of the role of transparency in the acceptance of ELM. Transparency is defined as the extent to which employees are given information and notified about the characteristics of workplace monitoring (White et al., 2020). Since individuals are more likely to accept monitoring when organizations are transparent about the process involved in setting policies and procedures (Al-Jabri & Roztocki, 2015; Leventhal et al., 1980), transparency about the nature and purpose of monitoring is an important issue that needs further investigation (Brauneis & Goodman, 2018). In other words, although increasing transparency regarding tracking systems can increase people's willingness to adopt them (Porumbescu et al., 2020; Wu et al., 2021), too much transparency might be counterproductive. Making people aware of the operating principles and types of data gathered by the system could trigger privacy concerns and reduce employees' acceptance of being monitored. Privacy in the work context can be described using control theory, which measures privacy as the amount of control a person has over their personal information (Moor, 1990). Another approach is restricted access theory, in which privacy is characterized by the level of access others have to someone's personal information (Moor, 1997). In either case, with the advent of more invasive and ubiquitous monitoring systems due to increasing digitalization of the work environment, organizations are forced to reconsider their concept of employee privacy.To address this problem, this study analyzes how transparency regarding monitoring shapes the relationship between perceived privacy risk and the acceptance of ELM technology in the smart manufacturing context. In more detail, we pursue the following research aims: (1) to determine how the perceived privacy risk resulting from monitoring can be addressed,

(2) to identify the role of transparency regarding monitoring and perceived value, and (3) to define moderators of the relationship between acceptance of monitoring and perceived risk and privacy concerns. To achieve these aims, an experiment with 135 participants was conducted in a laboratory setting in which participants were exposed to a real work situation while being electronically monitored. Transparency was manipulated using two conditions: One group received a detailed explanation of the monitoring and what data was being collected, whereas the other group did not receive any information about how the monitoring data would be processed during the experiment (but was informed after the experiment). After carrying out the work tasks, participants were asked about their acceptance of surveillance, their privacy concerns, perceived risk, and perceptions of monitoring to investigate how these interact with acceptance of EM. This enabled us to identify the role of transparency for acceptance of tracking and tracing systems. Many studies call for transparency when employing EM, while our study describes how transparency can be used properly to increase acceptance and what negative effects too much transparency may have. Our moderated mediation model of perceived value, transparency, perceived risk, privacy concern and acceptance of monitoring can serve as a foundation for future research in this context.This paper is structured as follows: Section 2 provides technical background on tracking and tracing systems and theoretical issues in EM, which are needed to develop the hypotheses. Section .1 describes the experimental setup, sample and measures. Finally, Section .2 presents the results of the hypothesis tests, and Section 2 discusses the results and provides recommendations for managerial practice. 2Theoretical background and hypotheses development.

1.1. Location-based services

Advances in technology such as intelligent surveillance give organizations with a constant overview of the business process by collecting various data that help to coordinate, plan and optimize production processes (Brettel et al., 2014). Location-based services are defined as services that take an entity's geographic location into account (Junglas & Watson, 2008). The tracking and tracing of physical objects is referred to as asset tracking and captures all activities and methods for capturing and using real-time locations and status data for objects, such as tools, containers, raw materials or production orders. It is already standard in many industries (Oztekin et al., 2010).

For the term location-based services to apply, four conditions must be met: First, the term 'entity' in this context refers to an object for which location information is stored, and can be either human or non-human. For instance, manufacturing good that is physically tracked on the shop floor for product and process quality purposes is a non-human object. Second, a location-based service always involves at least two entities. In a general geographic grid (e.g. longitude and latitude), entity A is always in relative position to entity B. Furthermore, each entity can be either static or in motion, where static may mean either permanently static (such as a building) or temporarily static (such as a parked truck). Third, one of the entities is always the object of location-based services, which means that position information for this object is recorded. Fourth and finally, one of the entities is always the receiver of the location information for the tracked object. The literature distinguishes between location-aware services and location tracking

services (Barkhuus & Dey, 2003). *Location-aware services* provide personal user information at a specific geographic location for users, whereas *location tracking services* provide information about user's whereabouts for platform operators. Usually, location tracking services are used for logistical purposes. Although it is more common for objects, humans can be tracked with the same technology, raising ethical issues.

The application of cyber-physical production systems in the context of smart manufacturing increases the amount of data collected through smart sensor technologies (e.g. wearables, IoT). These technologies promise increased productivity, operator support and real-time monitoring in an increasingly complex work environment, where simple repetitive tasks have been automated (Krishnamurthi et al., 2020; Ordieres-Meré et al., 2019). A key factor in the success of these technologies is the availability of data about the employee and his or her workplace and tasks. However, it is important to realize that the collection of such data about employees is not a trivial task, but rather a significant challenge for organizations in terms of meeting societal and legal requirements. To do so, it is necessary to ensure that the data obtained meet all requirements of secure and correct use by authorized persons only. It is essential for organizations to build employees' trust in the technology and the organization and to design these technical solutions in a way that has direct added value for them when using it, which could help to convince employees that the sharing of their data is crucial. For example, initial applications to analyse employee health data can help to identify health problems at an early stage and can thus suggest preventive measures (Austin et al., 2021). This can then reduce sick leave, which is beneficial for both employees and the organization. Furthermore, an increase in available data on employee behaviour can make it possible to more objectively assess individual performance, which can lead to a higher degree of fairness through fairer pay (Hancock et al., 2018).

Current asset tracking systems use wireless sensor networks to determine the position of an object (Khalaf & Sabbar, 2019). These systems are based on standardized wireless technologies that are also common in everyday life, such as Wifi, Bluetooth, RFID, or ZigBee (Zafari et al., 2019). Each object must be equipped with a tag or beacon, i.e. a radio transmitter. These tags are active or passive radio transmitters that send their identification number to a suitable system at a certain interval. Readers are statically positioned in the area where data recording takes place to ensure optimal detection of the radio signals from the tags. Figure 1 schematically illustrates the architecture of a TATS. Readers collect a transmitter's identification number and a received signal strength of its radio signal. Using triangulation, values from multiple readers can be used to calculate the physical location of a tag in the observed zone (Zafari et al., 2019).

1.2. Employee monitoring

Organizational control is dynamic and evolves over time (Cardinal et al., 2004). Many organizations may directly monitor employees' work or decide to use tools and systems such as monitoring and tracking technology. Although it might have beneficial outcomes for the organization (e.g. reducing costs, Jeske, 2021; optimizing performance by identifying room for improvement, Welter & Ensslin, 2021; monitoring quality and managing potential risks, White et al., 2020), ensuring that employees accept monitoring can be challenging.

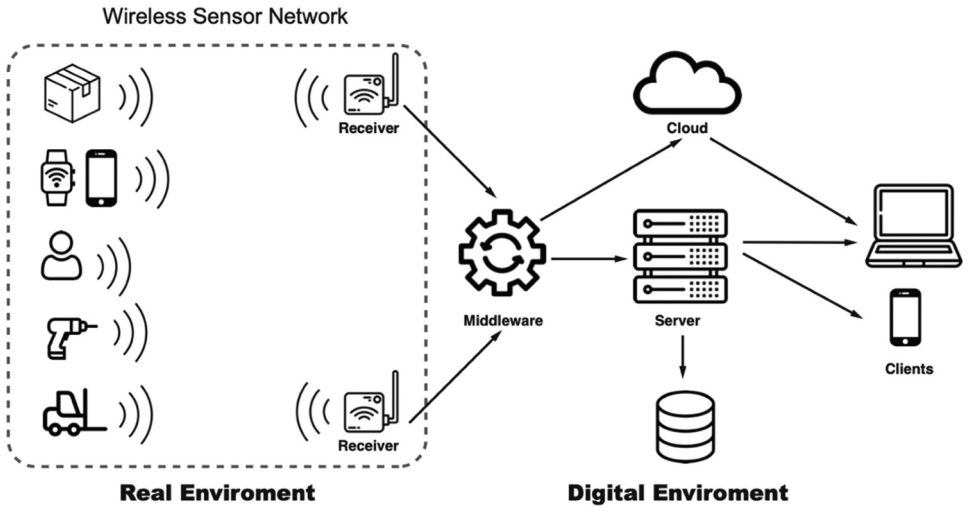

Figure 1. Exemplary system architecture of a tracking and tracing system (Jandl et al., 2021).

Holt et al. (2017) discusses the ethical implications of monitoring and found that people consistently rate the ethics of the organization poorly when it deploys a high level of monitoring. The important role of workers and the social subsystem for the adoption of Industry 4.0 technologies has been discussed (Marcon et al., 2022; Vereycken et al., 2021). Thus, implementing and successfully operating monitoring technologies requires acceptance by users before planning and implementations.

While the use of innovative tracking and tracing technologies holds attractive potential for companies, it is also associated with serious risks. There is considerable evidence in the literature that monitoring can also evoke negative reactions, such as feeling that one's privacy has been invaded (McNall & Roch, 2007), perceptions of unfairness (Moorman & Wells, 2003), decreased job satisfaction and organizational commitment (Wells et al., 2007) as well as greater stress in work-related tasks (Aiello & Kolb, 1995; Ravid et al., 2022). It is now well established from a variety of studies that the extent to which employees believe monitoring is an invasion of privacy influences their acceptance of monitoring (Alder et al., 2008; Van Slyke et al., 2006). Privacy concerns could be a significant barrier to the growth of ubiquitous technology, which collects and stores extensive information about people and their activities (Perera et al., 2016; ten Berg et al., 2019). If employees are expected to use a device that tracks their location and the time spent in each location, their privacy can be undermined, as this tracking serves as a proxy for information privacy. Information privacy is a subset of general privacy and reflects identifiable personal information (Smith et al., 2011).

While perceived privacy risk refers to potential losses resulting from sharing and disclosing information (ten Berg et al., 2019), we expect that individuals' perceived privacy risk is shaped by their general concern about privacy. Privacy is defined as 'a state or condition in which the individual has the capacity to (a) control the release and possible subsequent dissemination of information about him or herself, (b) regulate both the amount and nature of social interaction, (c) exclude or isolate him or herself from

unwanted (auditory, visual, etc.) stimuli in an environment, and, as a consequence, can (d) behave autonomously' (Stone & Stone, 1990, p. 358).

Generally, privacy-related decisions involve trades-offs and are based on individuals' 'privacy calculus,' that is, engaging in a cost-benefit analysis where they evaluate the perceived risks versus the perceived benefits of providing (or accessing) information (Dinev & Hart, 2006). Based on this calculus, people decide both consciously and unconsciously about the privacy they are giving up and the benefits they receive in return (Dinev & Hart, 2006). If the perceived benefits exceed the calculated risks to privacy, individuals will be more likely to react more favorably to monitoring. Thus, perceived risk is a more situation-based factor that can override the dispositional factor of general privacy concerns (Kehr et al., 2015). ten Berg et al. (2019) found that despite their privacy concerns, people are willing to disclose personal information when asked to comply. Zhou (2013) also found perceived privacy risk to inhibit usage intention. This deviation between reported privacy concerns and the intention to disclose personal information is known as the privacy paradox (Li & Sarathy, 2007; ten Berg et al., 2019). Thus, we assume that perceived risk resulting from the privacy calculus will mediate the negative association between privacy concerns and the acceptance of monitoring. Therefore, individuals should be more likely to accept monitoring when they perceive lower privacy risk in using monitoring technologies.

***H1**: Perceived privacy risk mediates the relationship between privacy concerns and the acceptance of monitoring.*

Transparency has been suggested as a general design recommendation to reduce resistance to monitoring (Abraham et al., 2019; Backhaus, 2019; Tomczak et al., 2018). ten Berg et al. (2019) found that the majority of participants have no or fewer problems with tracking when the collection and usage of data is transparent. Similarly, a meta-analysis of the effects of employee performance monitoring revealed that more positive employee attitudes can be expected when the organization's monitoring is more transparent (Ravid et al., 2022). Ambrose and Alder (2000) also found negative reactions to monitoring systems when employees do not know whether they are being monitored, why they are being monitored, or how they are being monitored.

Together, these studies show that negative impacts can be reduced when employers are transparent about monitoring. Ravid et al. (2022) describe transparency as the degree to which individuals have access to information regarding monitoring characteristics. Previous studies suggest that increasing transparency about the type of data collected and to what purpose could influence individuals' level of concern and disclosure attitudes (Chua et al., 2021). While Willford and colleagues (2015) found that individuals who did not know if they were being monitored provided the most negative ratings on measures of privacy invasion, Oulasvitra (2014) found that transparency about the intention of data collection reduces privacy concerns. Providing transparency can even help employees reach their goals (Locke & Latham, 2005) by providing feedback (Urbaczewski & Jessup, 2002) and could promote confidence and trust in the organization (Chua et al., 2021). Abraham et al. (2019) found that transparency about tracking and its use can lead to higher level of acceptance because it leads individuals to perceive higher control over

the content and use of tracking data. Thus, we consider transparency as a principle of work design that can support and accelerate the implementation of monitoring technologies. Demir et al. (2014) suggested that lack of transparency may undermine individuals' ability to effectively evaluate privacy risks associated with the collection and processing of their data. Thus, we argue that providing transparency helps individuals obtain a better understanding of monitoring technology, formulating our next hypothesis as:

***H2**: Transparency attenuates the negative effect of privacy risk on acceptance of monitoring.*

Recent studies (Schmidt et al., 2019; Tomczak et al., 2018) have proposed that improvident use of transparency can also have a negative effect on individuals' attitudes towards and acceptance of technology. The problem is that full transparency may reveal information that can intensify uncertainty about (the purpose of) monitoring. Therefore, it is important that organizations clearly communicate their reasons for adopting EM technology to offset the stress associated with uncertainty. Tomczak et al. (2018) suggested that organizations need to notify employees about monitoring instead of continually reminding them. While this method can be useful to avoid increasing stress perceptions, it does not ensure that the benefits of monitoring are understood by employees. Furthermore, Ravid et al. (2022) suggest that employees' perception of EM is more important than what is officially communicated to them.

Moreover, monitoring and collecting information about employees and their performance can have different purposes. Urbaczewski and Jessup (2002) found that people who were monitored electronically for feedback purposes have higher satisfaction with monitoring than those who were monitored for surveillance. In the feedback condition, data was used positively to help individual performance, but under the surveillance condition, the data was solely used to ensure compliance with rules and regulations. Therefore, the purpose of monitoring is important and might also influence employees' acceptance of monitoring. For example, when working in hazardous environments, employee monitoring systems can increase occupational safety (Kaupins & Minch, 2005), which is probably more accepted by employees than using tracking technologies to monitor performance (Ravid et al., 2022).

In accordance with the privacy calculus model, employees may accept monitoring when they understand how it will benefit them or the organization (Acquisti, 2009). Other studies have proposed a positive relationship between understanding the system and participants' intent to use the system (Cramer et al., 2008; Venkatesh et al., 2003). Thus, for transparency to have a positive effect, we suggest that individuals need to know what data is being collected and how, so that they can better understand the inputs used for decision-making. This is important so that employees can better perceive the value associated with it. Therefore, we assume that the beneficial effect of transparency is even stronger once the value of monitoring is considered.

***H3**: The beneficial moderating effect of transparency between privacy risk and acceptance of monitoring is particularly strong when the value of monitoring is perceived as high.*

2. Method

2.1. Procedure

We designed an experiment at the TU Wien's pilot factory for students enrolled in the course 'Fundamentals in Work Science' and manipulated transparency (high/low) about location-based monitoring during a practical task. The data was collected between July 2020 and May 2021. Participants in the experiment received participation points for their course at TU Wien, but could opt out of the experiment at any time or decide to have their data omitted from the experiment. Participants were asked to use 18 different parts (i.e. filament extruder, two stepper motors, extruder carriage with rails, metal housing parts) to assemble a 3D printer, guided by a worker assistance system. Each assembly station had a driverless transport system equipped with a screwdriver and Bosch Rexroth cordless screwdriver, and a shelving system with gripper boxes on a roller system that was equipped with all the required 3D printer components. Participants' location was monitored during this task using the ultrawide band tracking system from the vendor kinexion. The whole tracking location inside the factory consists of an area of 20 by 30 metres. In order to train and test the experimental procedure, several test runs were carried out beforehand. Each participant went through the following stations, which took a total of approximately 45 minutes per participant.

First, participants were welcomed by the experimenter into a closed area that blocked their view of the shop floor. There, participants were briefed about the experiment and signed the informed consent form. To standardize this step, participants received the basic instructions in the form of a recorded video with a fictitious scenario involving 'Future Print Corp.', a company that is seeking to optimize its assembly line for 3D printers. The video went through all steps of assembling the 3D printer, placing particular emphasis on how to operate the assistance system. At the end of the video, the participant was equipped with a tag to monitor their exact positioning with respect to the workstation. Depending on the experimental condition, the participant was either notified that the monitored data could be viewed after the task or not. The shop floor had two assembly stations, each equipped with a worker assistance system, that were used in parallel for the experiment. These were located next to each other but were separated by roll-ups. Participants had 20 minutes to complete the task. After these 20 minutes, the 3D printer in its current state was subjected to a quality check to determine whether it had been assembled correctly. After assembling of the 3D printer, half of the participants (experimental group = high transparency) received detailed information about the content and extent of information tracked during the assembly task. The other half of participants (control group) didn't receive any further information about the collected data. Subsequently, all participants filled out the questionnaire described in the measures section. Once the experimental sequence was completed, all participants received an e-mail with further information about the experiment and explaining that Future Print Corp. was fictitious.

2.2. Sample

A total of 148 undergraduate participants took part in this experiment. Of those, 13 participants were excluded for failing the manipulation check of transparency. Thus, the

final sample consisted of 135 participants (18% women and 82% men), ranging in age from 20 to 31 years (M = 22.35, SD = 2.16). The high percentage of male students reflects the current situation at TU Wien, but also in the field of study (i.e. mechanical engineering) in general and in the actual labor force in this field. The majority of respondents (88%) had no experience with location-based monitoring. Less than half of participants (44%) indicated having little knowledge about the topic of monitoring. At the beginning of the experiment, participants were randomly assigned to one of the conditions: 69 participants were assigned to the experimental group (i.e. high transparency about monitoring) and 66 participants to the control group (i.e. low transparency about monitoring).

2.3. Measures

The following measures were used in our experimental setting and administered via an online survey after the work task. The measures were Likert scales and all in the German language. They were constructed using a double translation procedure by two different researchers fluent in both German and English.

2.3.1. Transparency

refers to the degree to which individuals have access to information about monitoring White et al. (2020). To increase transparency, we informed participants about what personal data was being collected and how it would be used Cradock et al. (2017). A sample item was 'I was informed about what data was recorded from me during task completion'. It was measured with 3 items, all of which were rated on a 5-point Likert-type scale ranging from 1 (= strongly disagree) to 5 (= strongly agree). Cronbach's α was 0.92. We also used this measure for our manipulation check of the experimental condition.

2.3.2. Acceptance of monitoring

captures attitudinal beliefs about monitoring and was assessed via five items, three of which were adapted from Stanton (2000) and two of which were self-constructed. We checked whether these five items loaded onto a single factor in a factor analysis. A sample item was 'Future Print Austria should be allowed to monitor employees at the workplace'. All items were rated on a 5-point Likert-type scale ranging from 1 (= strongly disagree) to 5 (= strongly agree). Cronbach's α was 0.78.

2.3.3. Privacy concerns

describe individuals' general concerns about disclosing personal information. It was measured with 14 items from Stewart and Segars (2002) capturing concerns about data collection, unauthorized access, collecting inaccurate information, and secondary usage of personal data. A sample item was 'I am concerned that companies are collecting too much personal information about me'. All items were rated on a 7-point Likert-type scale ranging from 1 (= strongly disagree) to 7 (= strongly agree). Cronbach's α was 0.85.

2.3.4. Perceived privacy risk

refers to the uncertainty that one's personal data will be misused, resulting in damage (Dinev & Hart, 2006). It was measured with 4 items from Sun et al. (2015). A sample item

was 'Disclosing my location information to Future Print Austria may bring many unforeseen problems'. All items were rated on a 7-point Likert-type scale ranging from 1 (= strongly disagree) to 7 (= strongly agree). Cronbach's α was 0.74.

2.3.5. Perceived value

of monitoring captures individuals' calculated trade-off between benefit and risk. We used 3 items adapted from Xu et al. (2011). A sample item was 'I think the benefits gained from employee monitoring will be greater than the risks of privacy'. All items were rated on a 7-point Likert-type scale ranging from 1 (= strongly disagree) to 7 (= strongly agree). Cronbach's α was 0.79.

2.3.6. Interactional justice

describes whether individuals' personal needs were taken into account in the decision and whether adequate explanations were provided (Niehoff & Moorman, 1993). It was measured with 5 items from Niehoff and Moorman (1993). A sample item was 'When decisions were made about my tasks, I was treated with kindness and consideration'. All items were rated on a 7-point Likert-type scale ranging from 1 (= strongly disagree) to 7 (= strongly agree). Cronbach's α was 0.75.

Finally, participants were asked to indicate basic socio-demographic information such as age (in years), gender (0 = female, 1 = male), and previous experience with location-based monitoring systems (5-point scale) as well as previous knowledge about location-based monitoring systems (5-point scale).

3. Results

3.1. Preliminary data analysis

Confirming that the manipulation of transparency was successful, a t-test between the two groups showed a significant difference in scores for the experimental ($M = 4.15$, $SD = 0.84$) and control ($M = 2.42$, $SD = 1.04$) conditions; $t(133) = 10.59$, $p < 0.001$.

According to Table 1, the correlation between privacy concern and acceptance of monitoring was not significant ($r = -0.12$, $p = 0.18$). Perceived risk was correlated with acceptance of monitoring ($r = -0.32$, $p < 0.01$). That is, the higher the perceived risk, the lower the acceptance of the monitoring system. Perceived value was not significantly correlated with acceptance of monitoring ($r = 0.12$, $p = 0.15$). Furthermore, we found a weak correlation between transparency and perceived value ($r = 0.21$, $p < 0.05$) and a moderate correlation between transparency and interactional justice ($r = 0.44$, $p < 0.01$). As transparency increases, the perceived value of monitoring as well as perceived interactional justice increase. There was no evidence of a direct relationship between **transparency** and perceived risk ($r = -0.09$, $p = 0.28$) or acceptance of location-based monitoring ($r = 0.05$, $p = 0.57$).

3.2. Testing hypotheses

Our analysis goal in this study is to establish the contingent nature of the mechanism by which privacy concern exert its influence on acceptance of monitoring to estimate how

Table 1. Means, standard deviations, and correlations of our study variables * $p < 0.05$, ** $p < 0.01$.

	M	*SD*	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.
1. Acceptance of monitoring	3.52	0.80	1									
2. Privacy concerns	5.32	0.91	−0.12	1								
3. Perceived privacy risk	4.02	1.26	−0.32**	0.37**	1							
4. Perceived value	4.12	1.47	0.12	−0.02	−0.09	1						
5. Transparency	3.31	1.28	0.05	0.01	−0.09	0.21*	1					
6. Interactional justice	5.65	1.09	0.09	0.10	−0.13	0.10	0.44**	1				
7. Age	22.35	2.15	− 0.09	−0.05	0.09	0.07	0.11	−0.04	1			
8. Gender	0.82	0.38	−0.15	0.01	0.05	−0.03	−0.07	−0.11	0.00	1		
9. Previous experience with monitoring	3.87	0.61	−0.16	0.00	−0.05	−0.15	−0.18*	0.01	−0.13	−0.10	1	
10. Previous knowledge about monitoring	2.05	0.82	0.12	−0.02	−0.05	−0.03	0.08	−0.00	0.08	0.05	−0.31**	1

this effect varies as a function of moderators. In other words, the indirect effect of privacy concern could be conditional on the extent of transparency and perceived value of monitoring. This can be accomplished by combining parameter estimates from a mediation analysis as well as a moderation analysis in ways that quantify the conditionality of various paths of influence from privacy concern to acceptance of monitoring.

For the hypotheses the PROCESS macro model scripts by Hayes (2013) were used. Those scripts are a set of macros, called PROCESS, usable in SPSS and SAS. PROCESS is a computational tool for observed variable path analysis-based moderation and mediation analysis as well as their integration as conditional process analysis. Further, the scripts can generate direct and indirect effects in mediation models, conditional effects in moderation models, and conditional indirect effects in conditional process models with single or multiple mediators.

For H1, the PROCESS macro model 4 SPSS script was used (Hayes, 2013). The results were tested using 1000 bootstrapped samples and 95 percent confidence intervals. Privacy concern was the predictor variable, with perceived risk as the mediator. The outcome variable was acceptance of monitoring, as shown in Figure 2. Age, gender and interactional justice were entered as covariates.

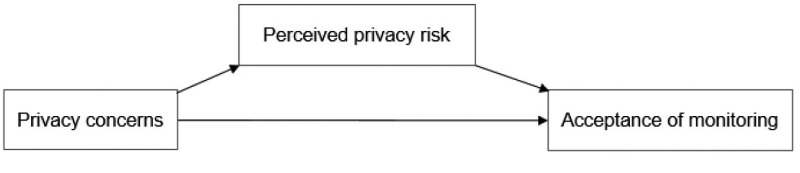

Figure 2. Mediation model of perceived risk, privacy concern and acceptance of monitoring.

The results revealed a significant indirect effect of privacy concern on acceptance of monitoring (unstandardized interaction B = −0.10, BSe = 0.04, 95% CI = −0.20 – −0.04). Furthermore, the direct effect of privacy concern on acceptance of monitoring was not

significant in the presence of the mediator (unstandardized B = −0.01, BSe = 0.08, t = −0.08, 95% Cl = −0.16–0.15). This indicates that perceived risk completely mediates the relationship between privacy concern and acceptance of monitoring. Thus, H1 is confirmed.

For H2, the PROCESS macro model 14 SPSS script was used (Hayes, 2013). The results were tested using 1000 bootstrapped samples and 95 percent confidence intervals. Privacy concern was the predictor variable, with perceived risk as the mediator and Transparency was the mediator, as shown in Figure 3. The outcome variable was acceptance of monitoring. Age, gender and interactional justice were entered as covariates.

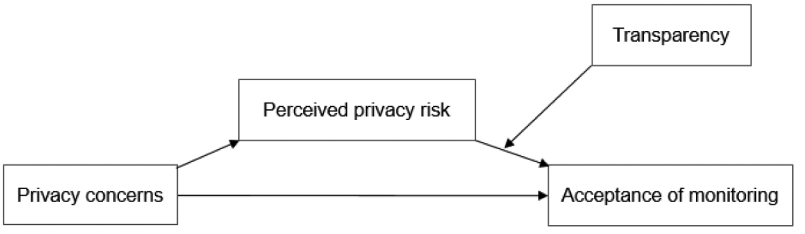

Figure 3. Moderated mediation model of transparency, perceived risk, privacy concern and acceptance of monitoring.

Transparency did not moderate the effect of perceived risk on acceptance of monitoring (unstandardized interaction B = 0.00, Bse = 0.04, t = 0.08, p = 0.94). The overall moderated mediation model was not supported, with the index of moderated mediation of 0.00 (95% CI = −0.05–0.06). As zero is within the CI, this indicates no significant moderating effect of transparency on the indirect effect of privacy concerns via perceived risk on acceptance of monitoring. Thus, H2 was not supported.

For H3, the hypothesized moderated mediation model was tested in a single model using the PROCESS macro model 18 SPSS script (Hayes, 2013). The results were tested using 1000 bootstrapped samples and 95 percent confidence intervals. Privacy concern was the predictor variable, with perceived risk as the mediator. The outcome variable was acceptance of monitoring. Transparency and perceived value were the proposed moderators, as shown in Figure 4. Age, gender and interactional justice were entered as covariates.

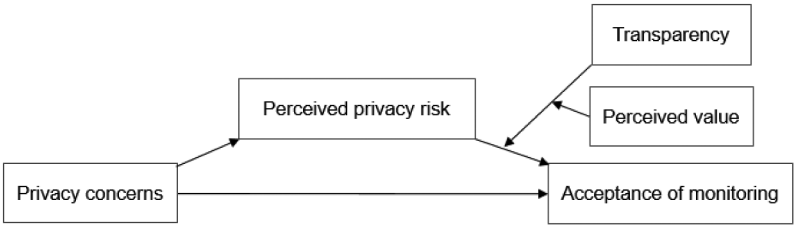

Figure 4. Moderated mediation model of perceived value, transparency, perceived risk, privacy concern and acceptance of monitoring.

Transparency was found to moderate the effect of perceived risk on acceptance of monitoring (unstandardized interaction B = −0.34, Bse = 0.09, t = −3.74, $p < 0.001$). Perceived value was also found to moderate the effect of transparency on perceived risk and acceptance of monitoring (unstandardized interaction B = 0.08, Bse = 0.02, t = 3.85, $p < 0.001$). The overall moderated mediation model was supported, with the index of moderated mediation of 0.05 (95% CI = 0.02–0.09). As zero is not within the CI, this indicates a significant moderating effect of transparency and perceived value on the indirect effect of privacy concerns via perceived risk on acceptance of monitoring.

When perceived value of monitoring is low, higher transparency increases the negative effect of risk on acceptance of monitoring. However, if the perceived value is high, increasing transparency reduces the negative effect of risk on acceptance, so that the relationship is no longer significant (perceived value = 5.59, transparency = 4.59, effect = 0.00, SE = 0.04, 95% CI = −0.08–0.09). This result implies that providing transparent information about monitoring is only beneficial when the perceived value is high. Thus, H3 was supported.

4. Discussion

Understanding the implications of location-based monitoring has significant influence on the design, deployment, and ultimately the success of future tracking systems. Despite its potential for improving employees' work processes, monitoring introduces many conflicts and concerns between employees and employers (Abraham et al., 2019). Prior studies have noted the importance of transparency in employee tracking (Schmidt et al., 2019; Tomczak et al., 2018); however, many uncertainties remain about the role of transparency in supporting or undermining employees' acceptance of the adoption of these technologies. The present study investigated how transparency about monitoring shapes the relationship between perceived privacy risk and the acceptance of location-based monitoring technology. We used an experimental setting with students and randomly assigned participants to either a group with high transparency (experimental group) or low transparency (control group) regarding monitoring.

Our results indicate that privacy concerns reduce individuals' acceptance of monitoring via perceived privacy risk. Consistent with the literature (e.g. Dinev & Hart, 2006; ten Berg et al., 2019), we found that privacy concerns and risks negatively affect the acceptance of monitoring. Furthermore, we found that transparency alone did not moderate the relationship between perceived privacy risk and acceptance. This finding has also been reported in public policy research (de Fine Licht, 2014; Grimmelikhuijsen, 2012), which has demonstrating that increased transparency does not necessarily generate trust and acceptance. According to the privacy calculus model, individuals will react more favorably to monitoring when they feel they have more to gain than the privacy they are losing/giving up (Acquisti, 2009). Once the perceived value of monitoring (i.e. the extent to which individuals valued the benefits vs. risks of monitoring) was taken into account, our results indicated that high transparency and high value combined were able to diminish the negative effect of perceived risk on acceptance of monitoring. This finding helps us better understand how individuals evaluate workplace practices that have the potential to violate privacy expectations. When the value was perceived to be low, being transparent about monitoring was found to backfire, and actually increased the negative effect of perceived

privacy risk. Taken together, these results suggest that organizations/decision makers cannot simply assume that providing transparency will increase adoption and acceptance; they also need to consider the value associated with the related technology when analyzing the consequences of increased decision-making transparency.

A theoretical contribution of our study is the creation and validation of an empirical model that explains how privacy concerns exert their impact on attitudes towards location-based monitoring. Our findings provide some support for the conceptual premise of an ambivalent relationship between transparency and privacy (Gierlich-Joas et al., 2022). We show that the relationship between privacy risk and transparency is not clear-cut and increasing transparency does not always decrease privacy risk. Our findings regarding the moderated effect of perceived value and transparency provide further insight into how organizations could encourage individuals to accept location-based monitoring. Consistent with the literature (Cramer et al., 2008; Venkatesh et al., 2003), we found that understanding the value of monitoring can prevent privacy risk from exerting negative effects on acceptance of monitoring when transparency is high. Previous studies have highlighted the importance of disclosing intentions for data use to users in an easily understandable manner (Anderson & Agarwal, 2011; Oulasvitra, 2014). That is, in order to diminish the negative effect of perceived privacy risk, individuals need to be aware of the purposes of monitoring, but also understand its value. However, our findings also show that perceived value alone is not sufficient; only together with increased transparency it is able to weaken the negative effect of perceived risk on acceptance of monitoring. While ensuring both transparency and perceived value will be beneficial, directing the user's attention to the benefits associated with monitoring will have a stronger effect than transparency alone. This may account for the mixed outcomes in prior empirical work on the effect of transparency on acceptance, in which perceived value was rarely taken into consideration.

Furthermore, the observed positive relationship between transparency and interactional justice is noteworthy. McNall and Stanton (2007) have shown that individuals' lack of control over location-based monitoring threatens their personal identity (privacy violation), which then affects their attitudes regarding the unfairness of monitoring. McNall and Roch (2007) found that informational justice partially mediated the relationship between transparency (providing an explanation for monitoring) and trust in management. Hence, it is conceivable that being transparent about monitoring can increase the perceived fairness of monitoring procedures.

The present findings underscore that transparency about monitoring needs to be provided strategically, in a way that allows the perceived benefits and value of monitoring to outweigh the perceived privacy risk. Based on our findings, while transparency is important, the effect of privacy risk on acceptance of location-based monitoring depends on the perceived value. Our finding broadly supports the work of Chang et al. (2015), who highlight the role of organizational culture in acceptance of employee monitoring by exploring the relationship between employees' privacy and trust. By providing justifications for implementing location-based monitoring, organizations can reveal that they care about their employees and that this is not just a way of exercising more control over them.

4.1. Managerial implications

This study has several managerial implications. Firstly, managers should pay much more attention to ensuring transparent communication with those who are being monitored. Integrating smart manufacturing technologies requires focusing on sociotechnical dimensions and conditions in order to ensure success (Marcon et al., 2022; Zafari et al., 2021). To ensure that employees are engaged in digital transformation processes and accept being monitored, organizations need to inform them about the rationale and reasons for monitoring. This should be communicated from the beginning of the implementation process to reduce resistance among employees.

As a second practical implication, organizations need to follow a method-driven rather than a technology-driven approach (Marcon et al., 2022) in which they first establish which benefits the data collected via monitoring should bring and then assess which technologies can serve these purposes. As privacy and transparency are interwoven in digital workplaces, managers should only monitor data that has a (transparent) purpose for both employees and employers and not monitor data merely for the sake of tracking and gaining control over employees, as the latter can lead to less compliance and commitment.

Finally, organizations need to be aware of how transparency about monitoring is communicated. That is, while transparency is important for gaining trust (Cradock et al., 2017), the negative effect of perceived risk on acceptance is stronger when transparency is high, but perceived value is low. Therefore, organizations opting for monitoring need to clearly communicate the benefits and value of monitoring so that the cumulative effects of perceived value and transparency outweigh perceived privacy risk to the point that it no longer prevents acceptance of monitoring. With this understanding, organizations can better communicate about monitoring to their employees to foster better understanding and prevent misconceptions about the purpose of monitoring.

4.2. Limitations and future research

The generalizability of these results is subject to certain limitations, creating a need for additional research. Firstly, we conducted our experiment with students, and female participants were less frequent in our sample than male participants. Therefore, the findings' external validity may be limited – although it is likely that the percentage of women working on the shop floor is low as well (e.g. only 25% of employees in manufacturing and production of goods in Austria are female (WKO, 2021)). Despite its limitations, our study can serve as an initial foundation for future studies with different demographic groups, including employees already working with tracking and tracing systems. However, the support for some of our theoretical predictions suggests that our experimental settings sufficiently resembled actual work settings to provide meaningful results. Furthermore, unlike employees, our student participants did not have to carry/fear any consequences during their work. That is, participants did not receive benefits if they performed the task faster or with better quality than others. It can be assumed that connecting performance appraisals to incentive schemes might affect acceptance of monitoring tools. More research is required to examine the effect of using performance data for rewards or punishments on acceptance of monitoring. Lastly, the

observed experimental work sequence was short and thus, the time participants were tracked was rather brief. During longer monitoring periods, however, individuals can experience many changes in technological systems and work processes. Thus, it would be interesting to examine perceptions (perceived value and privacy risk) about monitoring over time. Longitudinal research would help to address this concern and allow us to measure reactions to monitoring before, during, and after a monitoring system is introduced.

5. Conclusion

Location-based tracking technologies are rapidly being developed, and their implications for the workplace will increase. Central to Industry 4.0 and big data is the concept of transparency. While transparency about monitoring has been suggested as a general design recommendation, it is still not clear when transparency helps increase acceptance of monitoring and when it does not. Our empirical investigation showed that increasing transparency can sometimes backfire and negatively affect acceptance of monitoring. However, increased transparency together with high perceived value can diminish the negative effect of perceived risk on acceptance of monitoring. Moreover, we found that increasing transparency also promotes interactional justice. These results suggest that to increase acceptance of monitoring at workplaces, transparency needs to be adopted strategically in a way that allows the perceived value of monitoring to outweigh the perceived privacy risk. This highlights the need for careful communication about monitoring with employees.

Disclosure statement

No potential conflict of interest was reported by the author(s).

ORCID

Christian Jandl http://orcid.org/0000-0003-2430-0449
Setareh Zafari http://orcid.org/0000-0003-4940-1764
Martina Hartner-Tiefenthaler http://orcid.org/0000-0003-1597-3975
Sebastian Schlund http://orcid.org/0000-0002-8142-0255

References

Abraham, M., Niessen, C., Schnabel, C., Lorek, K., Grimm, V., Möslein, K., & Wrede, M. (2019). Electronic monitoring at work: The role of attitudes, functions, and perceived control for the acceptance of tracking technologies. *Human Resource Management Journal*, *29*(4), 657–675. https://doi.org/10.1111/1748-8583.12250

Acquisti, A. (2009). Nudging privacy: The behavioral economics of personal information. *IEEE Security & Privacy*, *7*(6), 82–85. https://doi.org/10.1109/MSP.2009.163

Aiello, J. R., & Kolb, K. J. (1995). Electronic performance monitoring and social context: Impact on productivity and stress. *The Journal of Applied Psychology*, *80*, 339–353. https://doi.org/10.1037/0021-9010.80.3.339

Alder, G. S. (2001). Employee reactions to electronic performance monitoring: A consequence of organizational culture. *The Journal of High Technology Management Research*, *12*(2), 323–342. https://doi.org/10.1016/S1047-8310(01)00042-6

Alder, G. S., Schminke, M., Noel, T. W., & Kuenzi, M. (2008). Employee reactions to internet monitoring: The moderating role of ethical orientation. *Journal of Business Ethics*, *80*(3), 481–498. https://doi.org/10.1007/s10551-007-9432-2

Al-Jabri, I. M., & Roztocki, N. (2015). Adoption of ERP systems: Does information transparency matter? *Telematics and Informatics*, *32*(2), 300–310. https://doi.org/10.1016/j.tele.2014.09.005

Ambrose, M. L., & Alder, G. S. (2000). Designing, implementing, and utilizing computerized performance monitoring: Enhancing organizational justice. *Research in Personnel and Human Resources Management*, *18*, 187–220.

Anderson, C. L., & Agarwal, R. (2011). The digitization of healthcare: Boundary risks, emotion, and consumer willingness to disclose personal health information. *Information Systems Research*, *22*(3), 469–490. https://doi.org/10.1287/isre.1100.0335

Austin, D., May, J., Andrade, J., & Jones, R. 2021. Delivering digital health: The barriers and facilitators to university-industry collaboration | Elsevier enhanced reader. *10* 1104–110. https://doi.org/10.1016/j.hlpt.2020.10.003

Backhaus, N. (2019). Context sensitive technologies and electronic employee monitoring: A meta-analytic review. *2019 IEEE/SICE International Symposium on System Integration (SII)*, 548–553. https://doi.org/10.1109/SII.2019.8700354

Barkhuus, L., & Dey, A. (2003). Is context-aware computing taking control away from the user? Three levels of interactivity examined. *International Conference on Ubiquitous Computing*, Berlin, Heidelberg, 149–156.

Bhave, D. P. (2013). The invisible eye? Electronic performance monitoring and employee job performance. *Personnel Psychology*, n/a-n/a. https://doi.org/10.1111/peps.12046

Brauneis, R., & Goodman, E. P. (2018). Algorithmic transparency for the smart city. *Yale JL & Tech*, *20*(1),103. https://doi.org/10.7282/00000058

Brettel, M., Friederichsen, N., Keller, M., & Rosenberg, M. (2014). How virtualization, decentralization and network building change the manufacturing landscape: An industry 4.0 perspective. *International Journal of Information and Communication Engineering*, *8*(1), 37–44.

Cardinal, L. B., Sitkin, S. B., & Long, C. P. (2004). Balancing and rebalancing in the creation and evolution of organizational control. *Organization Science*, *15*(4), 411–431. https://doi.org/10.1287/orsc.1040.0084

Chang, S. E., Liu, A. Y., & Lin, S. (2015). Exploring privacy and trust for employee monitoring. *Industrial Management & DataSystems*, *115*(1), 88–106. https://doi.org/10.1108/IMDS-07-2014-0197

Chua, H. N., Ooi, J. S., & Herbland, A. (2021). The effects of different personal data categories on information privacy concern and disclosure. *Computers & Security*, *110*, 102453. https://doi.org/10.1016/j.cose.2021.102453

Cradock, E., Stalla-Bourdillon, S., & Millard, D. (2017). Nobody puts data in a corner? Why a new approach to categorising personal data is required for the obligation to inform. *Computer Law & Security Review*, *33*(2), 142–158. https://doi.org/10.1016/j.clsr.2016.11.005

Cramer, H., Evers, V., Ramlal, S., van Someren, M., Rutledge, L., Stash, N., Aroyo, L., & Wielinga, B. (2008). The effects of transparency on trust in and acceptance of a content-based art recommender. *User Modeling and User-Adapted Interaction*, *18*(5), 455–496. https://doi.org/10.1007/s11257-008-9051-3

de Fine Licht, J. (2014). Policy area as a potential moderator of transparency effects: An experiment. *Public Administration Review*, *74*(3), 361–371. https://doi.org/10.1111/puar.12194

Demir, L., Cunche, M., & Lauradoux, C. (2014). Analysing the privacy policies of Wi-Fi trackers. *Proceedings of the 2014 Workshop on Physical Analytics - WPA '14*, 39–44. https://doi.org/10.1145/2611264.2611266

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, *17*(1), 61–80. https://doi.org/10.1287/isre.1060.0080

Gierlich-Joas, M., Teebken, M., & Hess, T. (2022). A synthesized perspective on privacy and transparency in the digital workplace. *Proceedings of the 55th Hawaii International Conference on System Sciences*, Manoa.

Grimmelikhuijsen, S. (2012). Linking transparency, knowledge and citizen trust in government: An experiment. *International Review of Administrative Sciences*, *78*(1), 50–73. https://doi.org/10.1177/0020852311429667

Hancock, B., Hioe, E., & Schaninger, B. (2018). *McKinsey Quaterly* (2). Accessed on 05 Aug, 2022. https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Organization/Our%20Insights/The%20fairness%20factor%20in%20performance%20management/The-fairness-factor-in-performance-management.pdf

Hayes, A. (2013). *Introduction to mediation, moderation, and conditional process analysis: A regression-based approach*. Guilford, New York.

Holt, M., Lang, B., & Sutton, S. G. (2017). Potential employees' ethical perceptions of active monitoring: The dark side of data analytics. *Journal of Information Systems*, *31*(2), 107–124. https://doi.org/10.2308/isys-51580

Jandl, C., Taurer, F., Hartner-Tiefenthaler, M., Wagner, M., Moser, T., & Schlund, S. (2021). Perceptions of using tracking and tracing systems in work environments. In F.-F.-H. Nah & K. Siau (Eds.), *HCI in business, government and organizations* (Vol. 12783, pp. 384–398). Springer International Publishing. https://doi.org/10.1007/978-3-030-77750-0_24

Jeske, D. (2021). Monitoring remote employees: Implications for HR. *Strategic HR Review*, *20*(2), 42–46. https://doi.org/10.1108/SHR-10-2020-0089

Jeske, D. (2022). Remote workers' experiences with electronic monitoring during Covid-19: Implications and recommendations. *International Journal of Workplace Health Management*, *15*(3), 393–409. https://doi.org/10.1108/IJWHM-02-2021-0042

Jeske, D., & Santuzzi, A. M. (2015). Monitoring what and how: Psychological implications of electronic performance monitoring. *New Technology, Work and Employment*, *30*(1), 62–78. https://doi.org/10.1111/ntwe.12039

Junglas, I. A., & Watson, R. T. (2008). Location-based services. *Communications of the ACM*, *51*(3), 65–69. https://doi.org/10.1145/1325555.1325568

Kaupins, G., & Minch, R. (2005). Legal and ethical implications of employee location monitoring. *Proceedings of the 38th Annual Hawaii International Conference on System Sciences*, 133a. https://doi.org/10.1109/HICSS.2005.388

Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus: Privacy calculus: Dispositions and affect. *Information Systems Journal*, *25*(6), 607–635. https://doi.org/10.1111/isj.12062

Khalaf, O., & Sabbar, B. 2019. An overview on wireless sensor networks and finding optimal location of nodes. *7* 31096–1101. https://doi.org/10.21533/pen.v7i3.645

Krishnamurthi, R., Kumar, A., Gopinathan, D., Nayyar, A., & Qureshi, B. (2020). An overview of iot sensor data processing, fusion, and analysis techniques. *Sensors*, *20*(21). https://doi.org/10.3390/s20216076

Leventhal, G. S., Karuza, J., & Fry, W. R. (1980). Beyond fairness: A theory of allocation preferences. *Justice and Social Interaction*, *3*(1), 167–218.

Li, H., & Sarathy, R. (2007). Understanding online information disclosure as a privacy calculus adjusted by exchange fairness. 28th International Conference on Information Systems, Montreal. 21, (pp. 14).

Locke, E. A., & Latham, G. P. (2005). Goal setting theory: Theory building by induction. *Great Minds in Management: The Process of Theory Development*, 128–150.

Lucas, J., Burgett, J., Hoover, A., & Gungor, M. (2016). Use oF ultra-wideband sensor networks to detect safety violations in real time. *ISARC. Proceedings of the International Symposium on Automation and Robotics in Construction*, Waterloo. *33*, (pp. 1).

Marcon, É., Soliman, M., Gerstlberger, W., & Frank, A. G. (2022). Sociotechnical factors and industry 4.0: An integrative perspective for the adoption of smart manufacturing technologies.

Journal of Manufacturing Technology Management, *33*(2), 259–286. https://doi.org/10.1108/JMTM-01-2021-0017

Martin, K., & Freeman, R. E. E. (2002). Some problems with employee monitoring. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.348040

McNall, L. A., & Roch, S. G. (2007). Effects of electronic monitoring types on perceptions of procedural justice, interpersonal justice, and privacy. *Journal of Applied Social Psychology*, *37*(3), 658–682. https://doi.org/10.1111/j.1559-1816.2007.00179.x

Moor, J. H. (1990). The ethics of privacy protection. *Library Trends*, *39*(1), 69–82.

Moor, J. H. (1997). Towards a theory of privacy in the information age. *ACM Sigcas Computers and Society*, *27*(3), 27–32. https://doi.org/10.1145/270858.270866

Moorman, R. H., & Wells, D. L. (2003). Can electronic performance monitoring be fair? Exploring relationships among monitoring characteristics, perceived fairness, and job performance. *Journal of Leadership & Organizational Studies*, *10*(2), 2–16. https://doi.org/10.1177/107179190301000202

Niehoff, B. P., & Moorman, R. H. (1993). Justice as a mediator of the relationship between methods of monitoring and organizational citizenship behavior. *Academy of Management Journal*, *36*(3), 527–556. https://doi.org/10.2307/256591

Ordieres-Meré, J., Villalba-Díez, J., & Zheng, X. (2019). ChallengeS and opportunities for publishing iiot data in manufacturing as a service business. *Procedia Manufacturing*, *39*, 185–193. https://doi.org/10.1016/j.promfg.2020.01.308

Oulasvitra, A. (2014). Transparency of intentions decreases privacy concerns in ubiquitous surveillance. *Cyberpsychology, Behavior, and Social Networking* 17(10). 607–623. https://doi.org/10.1089/cyber.2013.0585

Oztekin, A., Pajouh, F. M., Delen, D., & Swim, L. K. (2010). An RFID network design methodology for asset tracking in healthcare. *Decision Support Systems*, *49*(1), 100–109. https://doi.org/10.1016/j.dss.2010.01.007

Perera, C., McCormick, C., Bandara, A. K., Price, B. A., & Nuseibeh, B. (2016). Privacy-by-design framework for assessing internet of things applications and platforms. *Proceedings of the 6th International Conference on the Internet of Things - IoT'16*, 83–92. https://doi.org/10.1145/2991561.2991566

Porumbescu, G. A., Cucciniello, M., & Gil-Garcia, J. R. (2020). Accounting for citizens when explaining open government effectiveness. *Government Information Quarterly*, *37*(2), 101451. https://doi.org/10.1016/j.giq.2019.101451

Ravid, D. M., White, J. C., Tomczak, D. L., Miles, A. F., & Behrend, T. S. (2022). *A meta-analysis of the effects of electronic performance monitoring on work outcomes*. Personnel Psychology.

Schmidt, B., Kessler, L., Holroyd, C. B., & Miltner, W. H. R. (2019). Wearing a bike helmet leads to less cognitive control, revealed by lower frontal midline theta power and risk indifference. *Psychophysiology*, *56*(12). https://doi.org/10.1111/psyp.13458

Smith, D. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, *35*(4), 989. https://doi.org/10.2307/41409970

Stanton, J. M. (2000). Reactions to employee performance monitoring: framework, review, and research directions. *Human Performance*, *13*(1), 85–113. https://doi.org/10.1207/S15327043HUP1301_4

Stewart, K. A., & Segars, A. H. (2002). An empirical examination of the concern for information privacy instrument. *Information Systems Research*, *13*(1), 36–49. https://doi.org/10.1287/isre.13.1.36.97

Stone, E. F., & Stone, D. L. (1990). Privacy in organizations: Theoretical issues, research findings, and protection mechanisms. *Research in Personnel and Human Resources Management*, *8*(3), 349–411.

Sun, Y., Wang, N., Shen, X. -L., & Zhang, J. X. 2015. Location information disclosure in location-based social network services: Privacy calculus, bene?t structure, and gender differences. *52*, 278–292. https://doi.org/10.1016/j.chb.2015.06.006

ten Berg, K., Spil, T. A. M., & Effing, R. (2019). The privacy paradox of utilizing the internet of things and Wi-Fi tracking in smart cities. In Y. Dwivedi, E. Ayaburi, R. Boateng, & J. Effah

(Eds.), *ICT unbounded, social impact of bright ICT adoption* (Vol. 558, pp. 364–381). Springer International Publishing. https://doi.org/10.1007/978-3-030-20671-0_25

Tomczak, D. L., Lanzo, L. A., & Aguinis, H. (2018). Evidence-based recommendations for employee performance monitoring. *Business Horizons*, *61*(2), 251–259. https://doi.org/10.1016/j.bushor.2017.11.006

Urbaczewski, A., & Jessup, L. M. (2002). Does electronic monitoring of employee internet usage work? *Communications of the ACM*, *45*(1), 80–83. https://doi.org/10.1145/502269.502303

Van Slyke, C., Shim, J., Johnson, R., & Jiang, J. J. (2006). Concern for information privacy and online consumer purchasing. *Journal of the Association for Information Systems*, *7*(6), 1.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, *27*(3), 425–478. https://doi.org/10.2307/30036540

Vereycken, Y., Ramioul, M., Desiere, S., & Bal, M. (2021). Human resource practices accompanying industry 4.0 in European manufacturing industry. *Journal of Manufacturing Technology Management*, *32*(5), 1016–1036. https://doi.org/10.1108/JMTM-08-2020-0331

Wells, D. L., Moorman, R. H., & Werner, J. M. (2007). The impact of the perceived purpose of electronic performance monitoring on an array of attitudinal variables. *Human Resource Development Quarterly*, *18*(1), 121–138. https://doi.org/10.1002/hrdq.1194

Welter, L. M., & Ensslin, S. R. How do the unintended consequences of performance evaluation systems manifest themselves?. (2021). *Journal of Accounting & Organizational Change*, *18*(4), 509–528. *ahead-of-print*(ahead-of-print. https://doi.org/10.1108/JAOC-07-2020-0087

White, J. C., Ravid, D. M., & Behrend, T. S. (2020). Moderating effects of person and job characteristics on digital monitoring outcomes. *Current Opinion in Psychology*, *31*, 55–60. https://doi.org/10.1016/j.copsyc.2019.07.042

Willford, JC, Howard, RH, Cox, MJ, Badger, JM, Behrend, TS 2015 A latent class analysis of electronic performance monitoring practices 30th Annual Conference of the Society for Industrial and Organizational Psychology Philadelphia, PA

Wu, W., Wu, Y. J., & Wang, H. (2021). Perceived city smartness level and technical information transparency: The acceptance intention of health information technology during a lockdown. *Computers in Human Behavior*, *122*, 106840. https://doi.org/10.1016/j.chb.2021.106840

Xu, H., Xin Robert, L., Carroll, J. M., & Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision Support Systems*, *51*(1), 42–52. https://doi.org/10.1016/j.dss.2010.11.017

Zafari, F., Gkelias, A., & Leung, K. K. (2019). A survey of indoor localization systems and technologies. *IEEE Communications Surveys & Tutorials*, *21*(3), 2568–2599. https://doi.org/10.1109/COMST.2019.2911558

Zafari, S., Köszegi, S., & Filzmoser, M. (2021). Human adaptation in the collaboration with artificial agents. In J.Fritz, N.Tomaschek (Eds.), *Konnektivität Über die Bedeutung von Zusammenarbeit in der virtuellen Welt*. 97–106. Waxmann Verlag GmbH. http://hdl.handle.net/20.500.12708/30581

Zhou, T. (2013). Examining continuous usage of location-based services from the perspective of perceived justice. *Information Systems Frontiers*, *15*(1), 141–150. https://doi.org/10.1007/s10796-011-9311-3

Zweig, D., & Webster, J. (2003). Personality as a moderator of monitoring acceptance. *Computers in Human Behavior*, *19*(4), 479–493. https://doi.org/10.1016/S0747-5632(02)00075-4