Privacy in a Digitized Workplace: Towards an Understanding of Employee Privacy Concerns

Mena Angela Teebken
LMU Munich
teebken@bwl.lmu.de

Thomas Hess
LMU Munich
thess@bwl.lmu.de

Abstract

When employees are required to work remotely, the digitization of the workplace becomes imperative to organizations. The introduction of digital workplaces leads to challenges and potentially negative consequences for employee privacy. Research did not yet shed light on the issue of employee privacy concerns. Therefore, the goal of this study is to evaluate the concept of privacy concerns in the context of the digitized workplace. Within the scope of this study, we conducted 33 semi-structured interviews with employees in order to gain insights into their Workplace Privacy Concerns (WPCs). Based on an iterative thematic analysis approach, we identified eight dimensions of WPCs: Six of these dimensions are adapted from the consumer context, two further dimensions represent concerns exclusive to the workplace context. This study serves as a starting point towards an understanding of WPCs and future research on the digitized workplace.

1. Introduction

The pandemic crisis is having a profound impact on the working world. To operate effectively, organizations must digitally transform their places of work. During this phase of reorganization, digital technologies play a key role. Technologies for communication and collaboration are essential to keep work operations running smoothly. In this regard, digitalization refers to the introduction of new solutions based on digital technologies, while digitization relates to the conversion from analog to digital [1]. Central for organizations to get through such a crisis without sustaining major losses is to step up their pace of digital transformation towards a digitized workplace where employees can work independently of their location. Beyond the crisis, recent remote work regulations serve as an accelerator to a transformation, which has already been advancing at speed: The digitization of the workplace. The "dark side" (p. 161) of the increasing use of information technologies (IT) embodies various negative phenomena that affect individuals as well as organizations [2], such as the loss of privacy at work. The increasing role of digital technologies challenges the concept of privacy, raising concerns that did not previously exist. The reason for that is the collection of user data on a large scale and growing capabilities to analyze data [3]. How does this digitization of the workplace affect the employees? Knowing that digital technologies constantly collect and process information, which privacy concerns do employees have in this new setting?

User privacy concerns are based on the "growing art of the possible" (p. 990) and are triggered by the growing options to collect, process, distribute and use personal information [4]. Thereby, privacy concerns deal with the individual's perception of what will happen to their data once they reveal it to another party [5]. Fueled by the vast expansion of digital technologies, the ease of collection, analysis and transfer of personal information, privacy-related issues are a common topic of interest in IS research [4, 6]. The concept of privacy concerns was operationalized by several studies. At the same time, these studies naturally assume the user of digital technologies to be a private consumer, leading us to the question: What are the context-specific privacy concerns of employees in their digitized workplace? Although workplaces are becoming digital at vast pace, the concept of WPCs has not yet been studied extensively. The focus of this study is the imperative consequence of workplace digitization: WPCs of employees. Due to practical and theoretical relevance, it is essential to understand those concerns. Therefore, the research questions of the study are the following: *"What are the dimensions of workplace privacy concerns?"* and *"Which factors have an impact on those workplace privacy concerns?"*

Current trends advance the amplitude of "dark side phenomena" (p. 161) [2], as IT-enabled activities produce data in vast amounts. Therefore, digital

URI: https://hdl.handle.net/10125/71420
978-0-9981331-4-0

technologies bring the “sharpest thrust” (p. 129) to shed light on workplace privacy issues [7]. To date, there has been a lack of research on the effect that digitalization has on the workplace context, especially on privacy issues [7]. Because of the “contextual nature of privacy” (p.1002) [4], the applicability of established theories needs to be re-evaluated in light of context-specific characteristics [8]. The conceptual basis of this study is drawn from Hong and Thong [9]. Their *Internet Privacy Concern* (IPC) scale includes the six most popular dimensions of consumer privacy concerns rooted in prior research. We choose a qualitative research approach to address the explorative research questions. Accordingly, we use semi-structured interviews to gain an understanding of WPCs. The findings of this study are two-fold: First, already established dimensions of privacy concerns are adapted to fit the workplace context. Second, two additional dimensions, namely *Employment* and *Private Device Usage*, are created to reflect privacy concerns specific to the workplace context.

2. Theoretical background

Literature recognizes two types of privacy: physical privacy and information privacy [10]. The former deals with physical access to the individual or their surroundings, while the latter concerns access to an individual’s personal information [10]. In Management Information Systems research, information privacy is defined as an individual’s ability to control what kind of personal information is collected, when and how it is collected and how it is used [11].

The concept of privacy concerns

In the past, there have been many attempts to conceptualize information privacy concerns. The concept of information privacy concerns is shaped by Smith et al. [10], who were among the first to express consumer privacy concerns in the *Concern for Information Privacy* (CFIP) scale. The CFIP scale is the most popular scale when it comes to measuring consumer privacy concerns [4]. Malhotra et al. [12] extended the CFIP scale to match the online context. The authors summarize their findings in the *Internet Users’ Information Privacy Concerns* (IUIPC) scale. Most studies that incorporate the concept of privacy concerns use either the CFIP or the IUIPC scale.

The CFIP is composed of the four dimensions *Collection, Errors, Secondary Use* and *Unauthorized Access* to Information. Firstly, the *Collection* dimension expresses the individual’s concern that extensive amounts of user data are compiled by organizations. *Unauthorized Secondary Use* describes the concern that information is collected for one particular (disclosed) purpose but is then used for another secondary purpose. *Improper Access* describes the user’s concern that unauthorized parties will be able to access confidential data. Lastly, *Errors* deals with the user’s concern that their personal information stored could contain deliberate or accidental errors.

Furthermore, the IUIPC scale identifies the three dimensions *Collection, Control* and *Awareness*, whereas the former is adapted from the CFIP. The *Control* dimension deals with the user’s ability to have control over their personal information, such as the option to opt-out of a service. *Awareness over Privacy Practices* deals with the user’s knowledge of how the company uses their data.

Hong and Thong [9] revisited the concept of information privacy concerns with the aim to consolidate prior literature towards a consistent construct. The authors combine the CFIP and IUIPC scales to create the six-item *Internet Privacy Concerns* (IPC) scale that includes the six most popular dimensions of privacy concerns: The first four dimensions are affiliated with the CFIP scale, and the two remaining dimensions stem from the IUIPC scale. Table 1 summarizes the IPC-concept of privacy concerns.

Table 1. Established dimensions of privacy concerns specific to the consumer context

IPC	CFIP	IUIPC
Collection	X	X
Errors	X	
Secondary Use	X	
Unauthorized Access	X	
Control		X
Awareness		X

IPC: Internet Privacy Concerns [9] , CFIP: Concern for Information Privacy [10], IUIPC: Internet Users’ Information Privacy Concerns [12]

The IPC scale’s conceptualization is based on the *Multidimensional Developmental Theory (MDT)* [13]. The MDT postulates that an individual’s privacy concerns are the result of their environment, individual experiences and interpersonal interaction [14]. The *Interpersonal Interaction* dimension describes how privacy boundaries are formed through the interaction with other parties. As the bilateral relationship between individuals and another entity is the main assumption in privacy concerns, the Interpersonal Interaction dimension is most relevant to understanding consumer privacy concerns [9] and therefore is a core dimension of the MDT [13].

The concept of privacy concerns serves as a proxy for measuring privacy on an individual level [4].

Researchers usually seek to explain differences in levels of privacy concerns by investigating antecedents, like demographics. They also study the effect of privacy concerns on outcome variables, e.g. the consumer's willingness to provide personal information [11]. Information privacy concerns have yet exclusively been explored in a consumer setting. Nevertheless, the topic of privacy at work is gaining momentum. A contextualized instrument for WPCs in a workplace setting is needed as a basis for further research in order to investigate causal links between antecedents, privacy concerns and outcomes in the workplace context.

3. Methodology

The digitization of the workplace is gaining importance given the recent developments in remote work regulations and is advancing at a fast speed. Since these developments have not previously been researched in the specific context of the workplace, the qualitative research approach was chosen to get a thorough understanding of the emerging topic [15].

3.1 Data collection

For our interviews, we followed a purposive sampling approach, thereby covering a heterogeneous sample of participants in order to uncover common patterns among those [16]. Only those individuals who are currently employed were considered as potential candidates for an interview. Information on the participants is provided in Table 2. The sample includes 19 females and 14 males aged between 21 and 67 years. In order to achieve a variation in perspectives, we interviewed participants who encounter different degrees of digitized workplaces. On the one side, we interviewed employees who only recently encountered digital technologies in their workplace due to remote work regulations and usually work offline, e.g. teaching assistants. On the other side, we also interviewed employees who are fully acquainted with working remotely, e.g. consultants. Employees using their private devices for work tend not to regularly work from home, while those completely working with their company devices are explicitly equipped to do so. Only 67% of the interviewees are fully equipped with company-owned devices even though current remote work regulations oblige to work from home. Also, 9% of employees use a mixture of private devices and company-owned devices (Hybrid). Within the scope of this study, the status of the working device serves as an indicator of the degree to which the workplace is equipped for its employees to work remotely.

Similar to the studies on the CFIP, IUIPC and IPC scales [9, 10, 12], this study does not focus on a specific technology in the workplace. Instead, the goal of the study is to gain a general and broad understanding of WPCs as a basis for further research. In order to get insights into the employees' privacy concerns, we conducted 33 semi-structured interviews with open-ended questions [17]. The interviews were held one-on-one on the telephone or via video-chat in the period from April to June 2020. We collected data until reaching saturation [18]. The study was conducted in Germany and the interviews were done in either German or English.

The interviews consisted of three parts. First, we asked the interviewees about their current use of digital technologies in their everyday work. This includes digital technologies that are used for working in-office as well as those used when working remotely. Second, we asked the interviewees about their usage habits of those digital technologies for work and their corresponding privacy concerns. In the next step, we asked the employees about their privacy concerns they would have if their workplace was fully digitized.

Table 2. Information on sample of participants

Age	**Frequency (Percentage)**
21-29	25 (76%)
>30	8 (24%)
Gender	**Frequency (Percentage)**
Female	19 (58%)
Male	14 (42%)
Working device	**Frequency (Percentage)**
Company-owned	22 (67%)
Hybrid	3 (9%)
Private	8 (24%)

3.2 Data analysis

We analyzed the interviews based on the iterative thematic analysis approach [19], which is an established method in qualitative data analysis. In the past, this approach has been successfully applied to uncover privacy concerns where sensitive consumer data is revealed, e.g. in the health context [20]. Prior research on consumer privacy concerns serves as a starting point for the exploration of privacy concerns in the workplace context. This study's conceptual basis is drawn from the IPC scale, which consolidates the most relevant dimensions of privacy concerns from the consumer perspective [9]. Together with the interview data, both serve as an input for the coding of the interviews. Interviews were conducted, transcribed and analyzed according to qualitative coding standards [15] by using Atlas.ti. Thereby, two researchers independently coded the data and the findings were jointly derived based on a condensed consensus. We constantly matched interview codes, factors and dimensions while reviewing literature. In a first step, we transcribed the interviews and recognized patterns in the data. By identifying recurring patterns in the transcripts, we generated 52 initial codes. In the next steps, these codes were grouped into factors and factors were grouped into dimensions. Statements that matched the IPC framework were coded deductively, while statements that could not be matched with already established dimensions were coded inductively. For instance, interviewees voiced their concerns about communication via video-chat. First, interviewees are concerned that they do not have a right to choose which service provider they use. Second, they are concerned that they do not have a choice about what features they want to use, e.g. whether they turn on their camera. We coded these concerns as *No Choice to Opt-Out* and *No Control over Usage of Features*. Under the review of existing literature, we combined both codes to produce the *Forced Acceptance* factor, which was then sorted to the *Control* dimension. The process of creating codes, matching them to factors and matching those factors to dimensions was constantly accompanied by reviewing the previously identified relevant pieces of literature. As a result of the thematic analysis, we identified eight dimensions of consumer concerns and 21 corresponding factors. The first six dimensions stem from consumer privacy research and are therefore adapted to the workplace context. The following two dimensions *Employment* and *Private Device Usage* were created for the workplace context and have not previously been identified in privacy research.

4. Findings

The emerging dimensions of privacy concerns are illustrated in Figure 1, corresponding factors influencing those dimensions are structured in Table 3. The first outcome of the study is the adaption of the six-dimensional IPC scale to the workplace context. Second, two additional dimensions are created to highlight privacy concerns specific to the workplace context.

4.1. Adapted concept of privacy concerns

Collection

The *Collection* dimension describes the user's concern that large amounts of their personal data are collected and then stored in databases [10].

Full transparency of the employee: One of the most pressing concerns that employees have is the notion of them becoming fully transparent towards the employer and third parties: "*You get really transparent as an employee and everything that you are doing is basically collected in terms of data*" [P7].

Data storage: In terms of data storage, employees are concerned about how long their data is stored. For instance, if teaching assistants hold online lectures that are recorded on video, the employee *"wouldn't really be willing to have those data [stored] forever*" [P21]. Another aspect of data storage is the concern of data being "*lost on the way"* [P20] or not being stored appropriately.

Intellectual Property (IP) Protection: When working remotely, there can be a need to store sensitive information in a shared drive that others can access. Employees who deal with their intellectual property at work can be concerned about the security of their digitized ideas: *"When the server is not guaranteeing a high confidentiality and if I am very concerned about maybe it can be leaked somehow, then my whole work can be influenced"* [P21].

Unauthorized secondary use

The dimension of *Unauthorized Secondary Use* describes the user's concern that data is collected for one declared reason but is then used for another secondary reason [10].

Recording of conversations: One of the most pressing concerns is the recording of communication, which represents a novel problem to the online context. Employees fear that "*every word you are saying is taken for granted, so that they [the conversation partner] may record it*" [P7].

Giving away data: Employees were also concerned about what happens to the information recorded during online conversations, as the recipient might "*try to use it in other terms*" [P7] or *"use it for whatever they want"* [P7]. They are also concerned about collected data being sold to third parties or private data being published.

Recruiting process: During application processes, a vast amount of data on the applicant is collected and analyzed. This includes not only explicitly revealed data but also implicitly collected data like the applicant's performance during online tests. This leads to the concern that "*it feels like this kind of data is kind of a reference point for your performance, probably also for the future*" [P28] or is a *"reference point also (...) for future performance evaluations"* [P28].

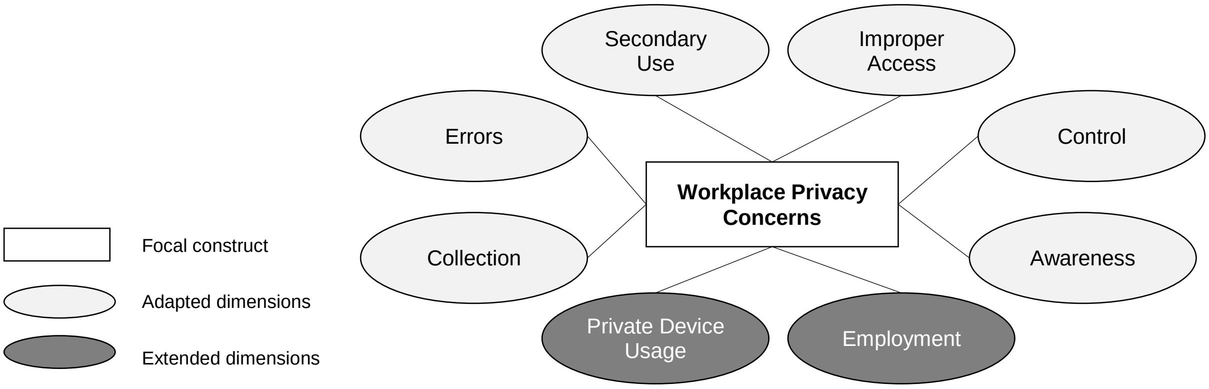

Figure 1: Dimensions of workplace privacy concerns

Errors

The *Errors* dimension includes the employee's concern that there is no adequate protection against deliberate or accidental errors in data collection [10]. Interpretatively in the workplace context, the Errors dimension deals with the concern that collected data on the employee is stored or interpreted inadequately.

Misinterpretation of offline-online status: One of the biggest and most pressing concerns of employees is the potential misinterpretation of their offline/-online status. This piece of information can lead to the misleading interpretation that the user is always working when they are online and never working when they are offline. Employees state that *"maybe I'm offline at one point and then they think she is not working at all but it's just because I am offline and not sitting in a team room"* [P7]. Therefore, employees are concerned that the online status could give a false signal about their productivity.

Misinterpretation of quantification: Another aspect linked to the online status is the quantification of working behavior. Employees feel as that various aspects of their working life are quantified. Such a quantification might not represent the quality of their work performance. They rather would prefer the employer *"to look more on output rather than […] on invested time or anything else"* [P19].

Improper access

The *Improper Access* dimension deals with the employee's concern that sensitive data might be improperly accessed by unauthorized parties [10]. Company internal: When employees use a common server to store their data and share it with colleagues, they are concerned about who will have access to this data. At the same time, they are concerned about colleagues, e.g. from the IT team, having remote access to virtually everything that they save on their device: *"I know that there is some form of admin user on the laptop as well. So, I am actually a little bit concerned about how much my company could look into what I am doing on my laptop"* [P19].

Third parties: On the other side, when using technologies provided by external service providers, employees are insecure about how these providers can access the data used in such services. Thereby, confidential company-data can be accessible to companies such as Google, who could then make use of the information. Employees are concerned that confidential data might be hacked in order to retrieve sensitive information: *"I am not sure if potential hackers could also get access to the cloud"* [P20]. Third parties with access to confidential data can also be customers with whom platforms are shared.

Control

The dimension *Control* describes the employee's concern that they cannot adequately control the collection of their personal information [12].

Forced acceptance: In the role of an employee, the user does not have the option or the ability to voice an opinion about whether they want to use the services of a provider and whether they want to reveal their private information. The statement *"then they told us to use it and then we did"* [P19] points out that the employees do not have a say about applications they use for work, even if they use them on their private devices.

Spread of digital content: When working at the office, the employee can, to some extent, keep conversations offline and discuss sensitive matters face-to-face. In a remote working situation, such face-to-face communication is replaced by digital means of communication: *"When you use such tools, there is a loss of control over contents"* [P12]. Those digital tools enable the recording and sharing of conversations and information in an easy and seamless way, without the sender's knowledge.

Protection of confidential data: What was already a challenge before is now more challenging in a fully digitalized workplace where also confidential data is digitalized. Connecting to the factor mentioned before, employees find it harder to protect confidential data from unauthorized access when the data is stored digitally. This leaves employees feeling that they are losing control: *"I am working with a lot of confidential information and data from my clients and I am not sure if this information is always in safe hands"* [P20].

Awareness of privacy practices

The *Awareness of Privacy Practices* dimension deals with the employee's concerns caused by the fact that they do not certainly know how collected data will be used by their employer or by third parties [12].

Internal handling of data: Employees know their employer can potentially use the information collected from their devices during work for further purposes. At the same time, they do not know whether and how much this is happening: *"I think one of the most pressing concerns is that the firm is actually collecting and using my data to some extent"* [P7]. Consequently, employees wish to have more information on what the employer is able to do with their workplace data.

Provider data handling: Service providers such as Google and Microsoft are known to collect user data, e.g. for analytical purposes. Users are "*concerned whether or how the companies really use the collected data*" [P33] for further analyses without them being informed.

Permission: This insecurity over how the employer and the service provider might handle the data is rooted in uncertainty about the employee's rights. For instance, this is shown by the fact that that users rarely read a complete data agreement and agree to any agreements in job contracts or prior to using a provider's services because "*everywhere you have that data agreements, wherever you go. And of course, people don't really read it. Or they just accept it*" [P19].

4.2 Extended concept of privacy concerns

Employment

The *Employment* dimension describes the degree to which employees are concerned that employers collect information that can be used to draw conclusions about the employee's productivity.

Fear of the future: With the growing popularity of AI, employees are concerned about companies using their data as an input for AI-enabled services. As a result, they are concerned about their work becoming redundant or obsolete. Ultimately, this leads to the concern that with growing capabilities of AI systems, their work will become worthless: "*they [tasks] could be automated so that my own personal work is redundant"* [P20]. This is ultimately leading to insecurities and concerns about job loss: "*I would be out of the job because computer programs would take over"* [P20].

Performance tracking: Collected working data can enable the employer to get a better understanding of the employee's performance on the job. This leads to the concern of employees that their data might be used to create employee profiles that display their productivity and efficiency. On top of that, they are concerned about employers consequently comparing them to their peers based on their quantified digital performance: *"my employer could develop a certain profile about my productivity at work, compare it with my peers and basically determine how well I perform when everything is digital"* [P20]. Employees fear that their performance, as measured through the system they use, does not correctly reflect the effort they put into their work or the quality of results.

Principal-Agent: Especially among younger interviewees, employees are concerned about the effects of increased transparency of their work performance when they are not acting in the company's best interest. On the one hand, employees might use company time and their company device for private purposes: *"It [the company laptop] is currently the best device in my household because it is newest. So, I am also using it randomly also for my private stuff"* [P19]. For instance, employees use their company laptops for "*looking up what food to order or watching some UK Netflix shows with the VPN"* [P3]. Employees are concerned that their employer can easily take note of any misbehavior or mistakes, which makes them concerned about negative consequences.

Private device usage

The *Private Device Usage* dimension describes the privacy concerns employees have over using their private devices for work.

Access to private data: When employees store private data and work-related data on the same device, they are concerned about their private data mixing up with their work: *"probably it could be that some of my private data from my private computer gets into the company space"* [P28]. They are also concerned about the employer having remote access to the private device. Therefore, employees perceive using their private device for work as an intrusion to their private life: *"it sometimes feels a little like you wouldn't necessarily have a private space, or like a safe space*" [P2].

Adequate storage of work-related data: When multiple users share one device, one concern employees have is whether they can accurately protect work-related data stored on their private device. In addition, employees feel that they cannot protect work-related data properly, as they are "*not sure if potential hackers could also get access to the cloud and hack these confidential details"* [P20]. They also fear the legal consequences of not storing company-related data accurately, e.g. confidential client data.

Table 3: Thematic table of workplace privacy concerns

Dimensions	Factors
Collection	Full transparency
	Data storage
	IP protection
Secondary Use	Recording of conversations
	Giving away data
	Recruiting process
Errors	Misinterpr. of offline-online status
	Misinterpretation of quantification
Improper Access	Company internal
	Third parties
Control	Forced acceptance
	Spread of digital content
	Protection of confidential data
Awareness	Internal handling of data
	Provider data handling
	Permission
Employment	Fear of the future
	Performance tracking
	Principal-agent
Private Device U.	Access to private data
	Adequate storage of work-related data

5. Discussion

Employees have the impression that greater digitalization threatens their right to privacy [7]. The study's findings show there is a broad range of privacy concerns among employees regarding the use of digital technologies at their workplace. In the following, we will first discuss the adapted concept of WPCs in contrast to IPC. Afterward, we will debate the emerging privacy concerns that are new to the workplace context.

5.1 Consumer versus employee privacy concerns

The study shows that the dimensions of consumer privacy concerns from the IPC can be well adapted to match the workplace context. In summary, the findings show that employees are concerned about the following aspects: (1) the collection of data in vast quantities, (2) the usage of data for secondary purposes that were not disclosed, (3) errors in the collection and interpretation of data, (4) improper access of sensible data by unauthorized parties, (5) a lack of control over whether and how to use technologies and (6) a lack of awareness of how their data will be used.

Two types of data are processed in a workplace context: The employee's personal data, which is explicitly or implicitly collected, and work-related data. Work-related data can, for instance, be confidential client data or sensitive company information. Thus, employees have the responsibility to keep different types of data safe. The results show that employees are not only concerned about their private data being mishandled, e.g. secondary usage by unauthorized users. Moreover, they are also concerned about protecting work-related data, e.g. when they need to store data on their private device safely. Hence, with a single data privacy breach, a vast amount of information could be revealed at once.

Another peculiarity of the workplace context is the vast amount of stakeholders that employees interact with. They engage in a relationship with not only a company providing service, e.g. Google, but also with work-related stakeholders, e.g. their colleagues, their superiors or their clients. For instance, interviewees were concerned that third parties would use the data collected by their provided services for further analysis. Additionally, they expressed their concern about colleagues improperly accessing their data. Furthermore, they were scared that their employers would replace their work with automated tasks or that customers could record them via video-chat. This shows that there are more potential touchpoints with other parties in a workplace context than in a consumer context. These touchpoints can lead to breaches of privacy and, therefore, to privacy concerns.

In their role as a consumer, users perform a cost-benefit analysis when they consider using a technology [21]. In such privacy-calculus models, consumers rationally weigh the anticipated risks of information disclosure against the potential benefits [22]. Same user, different context: Acting as an employee, the user cannot decide which technology to use. Ultimately, he cannot easily choose to switch employer if he has some concerns about his privacy practices.

Finally, in contrast to the consumer context, there is more at stake for employees if a privacy breach occurs. Ultimately, employees fear losing their job, which ties into the most existential concerns in human nature, namely their safety needs [23].

Within the scope of the study, the factors that influence dimensions related to the IPC-scale have been adapted to the workplace context. At the same time, we found out that the privacy concerns of employees exceed those of consumers. WPCs differ from IPCs in different aspects: Handled data, relevant stakeholders, a lack of a cost-benefit analysis and the outcomes of privacy breaches. To reflect these aspects, two dimensions concerning the employment relationship and the use of private devices are added, which apply specifically to the workplace setting.

5.2 Privacy concerns specific to the workplace context

While the interviewees presented a broad range of privacy concerns covering the dimensions of already established constructs, two additional dimensions were added that specifically address the workplace context: *Employment* and *Private Device Usage*. In the following, these dimensions are discussed in more detail.

The employer-employee relationship is vital to the employee, as they are to some extent dependent on their employer. At the same time, the increasing use of technologies at work leads to the ever-increasing transparency of the employee [7]. In turn, the increasing transparency leads to new opportunities in interpreting the employee's value-add to the firm. On the one side, employees are concerned that the increasing level of transparency can lead to the employer potentially observing them when they engage in inappropriate behavior, which can end in negative consequences. On the other side, employees are concerned about the quantification of their work and consequently, the employer quantifying their performance. They fear that such a quantification would not represent the effort they put into their work, e.g. when it comes to creative tasks. The ultimate fear of the employee is *The Fear of the Future*: Employees are increasingly concerned about their work data being collected and analyzed in a way that enables AI to replace them. Taken together, in the *Employment* dimension, employees are concerned about technology invading their working life and taking away their jobs.

Usually, employees acquainted with working from the office are not equipped with the tools to perform their work remotely. Therefore, they are often required to use their own and private devices when they need to work remotely. This leads to the employees having to install work-programs or save work-data on their private devices. Thereby, using one device for both private and professional matters, employees are at the one side concerned about their private data being at risk. On the other side, they are concerned about whether they are able to adequately store work-related data on their private device. Especially when employees share their device with other users, such as family members, they see the protection of work-data at risk. At the same time, they fear the consequences of potential data breaches when they are not able to protect data adequately. Using the same device for private purposes and for work purposes generates privacy concerns that did not exist before. Employees consider it an invasion of their private sphere if work enters their private device and whish for clear boundaries.

Taken together, a major cause of WPCs is the increasing technological development of the workplace. Further negative consequences of the increasing use of IT are manifested in a number of emerging phenomena experienced by individuals [2]. For instance, research shows that information and communication technologies lead to increased stress levels among their users [24]. This inability to cope with newly emerging technologies in a healthy way and the increasing stress level of employees due to the rise of information, communication and collaboration technologies is referred to as *technostress* [24, 25]. Employees suffering from technostress work more because others do not see them working, they feel pressured by the signaling of availability signs, they are concerned about being quantified and they are scared of technology taking over and, ultimately, replacing them. Besides the scope of information privacy concerns, employees express the concern of the blurring of boundaries between their private life and their work life. The following statement best represents this situation: *"I have a work-identity and a private-identity and right now these two are being mixed up a lot"* [P3]. The digitized workplace enables employees to work from any place at any time, which leads to the employees feeling pressured to really work from any place at any time.

The conceptualization of the IPC is based on the MDT, which describes privacy concerns emerging from the dyadic relationship between consumers and companies [9]. As this theory serves as a foundation for the IPC-construct, we believe it to be a suitable theoretical foundation for understanding the WPCs. In a workplace context, there is a dyadic relationship between the individual and company internal or external parties. The individual's privacy concerns in the workplace setting are caused by engaging with other parties that potentially collect and use their personal or work-related information. Therefore, the two work-related dimensions added to the IPC can be explained by the MDT's interpersonal interaction component. The interaction component relates to how individuals manage interactions with other parties and how the latter handle the individuals' personal information [9]. When employees use their private device for work, they are concerned about how well they are able to administer and protect their personal information and work-related data from unauthorized usage, leading to privacy concerns about the *Private Device Usage*. The *Employment* dimension is also directly related to the interaction dimension as it describes the employee's concern about data generated within their working relationships.

6. Conclusion

Despite the increasing role of digitalization at work, there is a lack of understanding of how workplace digitization causes employees to have privacy concerns. The goal of this study was to extend research on concerns over privacy in the emerging digitized workplace context. In order to understand the privacy concerns of employees, we conducted 33 semi-structured interviews and evaluated them by following an iterative thematic analysis approach. The derived thematic table (Table 3) consolidates WPCs and illustrates the broad range of concerns expressed by employees. The factor structure of the first six dimensions of the IPC scale (*Collection, Unauthorized Secondary Use, Improper Access, Errors, Control* and *Awareness*) was adapted to fit the workplace context. We added the two additional dimensions *Employment* and *Private Device Usage* to reflect additional concerns of users specific to the workplace context. One noteworthy dimension of concerns, which is not directly associated with information privacy, is the blurring of the boundary between private-life and work-life, which was a concern to the majority of interviewees.

6.1 Limitations

Using a purposive sampling approach, we interviewed 33 employees who currently work in a digitized workplace. The limited scope of interviewees leads to a limited external validity of research results. In regard to the purposive sampling approach, employees from different age groups, mixed genders, industry backgrounds and levels of digital maturity of working modes were interviewed to ensure a broad range of answers of respondents. Further research with different sampling methods is required in order to extend the generalizability of the study's findings.

Within the scope of the interviews, individuals employed in a digitized work context were invited to the study. Most of the study participants were younger than 30, as younger people tend to be better acquainted with working in a digitized workplace. Furthermore, employees – as well as users in general – often are not fully aware of what kind of data is collected, how it can be further analyzed, nor how this can affect them. Therefore, it can be beneficial to include older employee groups as well as the opinion of experts in future studies to learn more about WPCs.

6.2 Implications and outlook

Understanding the composition of WPCs is essential to developing appropriate measures to handle them. The thematic table (Table 3) can help employers recognize and address the privacy concerns of their employees. The results of the study show that employee privacy concerns are based on the "growing art of the possible" (p. 990) [4] and the lack of transparency about who does what with their digitized data. Employees do not know how their data is currently used by others, how it is potentially used, how much is collected, how it is collected, who can access it nor how it is quantified. Companies need to mitigate WPCs to enable a safe workplace for employees, where they feel less vulnerable to privacy breaches. At the same time, companies should enable a high level of data security, e.g. by protecting against unauthorized data usage or improper access. If remote working is continued in the future, companies need to invest in solutions that make employees feel more secure about working from their private device or even by providing them with portable work-devices. This is especially important if employees work with sensitive client data or confidential information. Moreover, in order to reduce concerns about the blurring of boundaries between private life and work-life and the feeling of technostress, managers need to implement explicit work norms to manage individuals' job expectations [24].

As a starting point for privacy research in the workplace context, the thematic table provides an overview of the dimensions of WPCs and corresponding factors. The next step in the conception of WPCs is to quantitatively test and validate the newly found dimensions and corresponding factors. After the conceptualization of the WPCs, research can further explore related antecedents and outcomes of privacy concerns, like how privacy concerns are shaped and how these concerns influence relevant workplace outcomes.

Technological innovations are transforming the structure and operations of organizations more than ever before [7]. For example, wearables can be used to increase productivity or ensure the safety and health of employees. Such devices carry a high risk of privacy invasion as they collect highly confidential employee data [7]. Thus, the increasing digitization of the workplace can be associated with a broad range of emerging phenomena corresponding to the "dark side" (p.161) of IT use [2]. Future avenues of research therefore should investigate the far-reaching implications of specific emerging technologies [7]. For instance, the increasing use of IT in the workplace context can lead to new security risks. In turn, tools to handle such security risks again potentially violate employee privacy [26].

The pandemic crisis has had an incremental impact on the digital transformation of workplaces. The imperative introduction and further development of digital working have the potential to transform communication and collaboration among employees without return. On the one hand, the digitized workplace can lead to productivity gains and increasing efficiency. On the other hand, digitization affects the employees of an organization. When a digitized workplace becomes the new normal, this leads to the question: What is the employee's perception of the digital workplace? More specifically, this paper sought to answer the question: Which privacy concerns do employees have in the digitized workplace? The answer is that employees have a variety of pressing privacy concerns, which can affect the way they perform their work. Therefore, it is essential to understand the drivers of employee privacy concerns in order to alleviate them and ultimately enable successful workplace digitization. The explorative design of this study serves as a starting point towards an understanding of WPCs in the digitized workplace. This study aims to provide a foundation for the topic of WPCs and to open up new avenues for research.

7. Bibliography

[1] Legner, C., Eymann, T., Hess, T., Matt, C., Böhmann, T., Drews, P., Mädche, A., Urbach, N., and Ahlemann, F., "Digitalization: opportunity and challenge for the business and information systems engineering community", Business and Information Systems Engineering, 59(4), 2017, pp. 301-308.

[2] Tarafdar, M., Gupta, A., and Turel, O., "Special issue on 'dark side of information technology use': An introduction and a framework for research", Information Systems Journal, 25(3), 2015, pp. 161-170.

[3] Ozdemir, Z.D., Smith, H.J., and Benamati, J.H., "Antecedents and Outcomes of Information Privacy Concerns in a Peer Context: An Exploratory Study", European Journal of Information Systems, 26(6), 2017, pp. 642-660.

[4] Smith, H.J., Dinev, T., and Xu, H., "Information Privacy Research: An Interdisciplinary Review", MIS Quarterly, 35(4), 2011, pp. 989-1015.

[5] Dinev, T., and Hart, P., "An extended privacy calculus model for e-commerce transactions", Information Systems Research, 17(1), 2006, pp. 61-80.

[6] Xu, H., Dinev, T., Smith, J., and Hart, P., "Information privacy concerns: Linking individual perceptions with institutional privacy assurances", Journal of the Association for Information Systems, 12(12), 2011, pp. 798-824.

[7] Bhave, D.P., Theo, L.H., and Dalal, R.S., "Privacy at work: A review and a research-agenda for a contested terrain", Journal of Management, 46(1), 2019, pp. 127 –164.

[8] Matt, C.T., Manuel; Cheung, Christy M. K.; Turel, Ofir, "The digitization of the individual: conceptual foundations and opportunities for research", Electronic Markets, 29(1), 2019, pp. 315–322.

[9] Hong, W.Y., and Thong, J.Y.L., "Internet privacy concerns: An integrated conceptualization and four empirical studies", MIS Quarterly, 37(1), 2013, pp. 275-298.

[10] Smith, H.J., Milberg, S.J., and Burke, S.J., "Information privacy: Measuring individuals' concerns about organizational practices", MIS Quarterly, 20(2), 1996, pp. 167-196.

[11] Bélanger, F., and Crossler, R.E., "Privacy in the digital age: A review of information privacy research in information systems", MIS Quarterly, 35(4), 2011, pp. 1017-1041.

[12] Malhotra, N.K., Kim, S.S., and Agarwal, J., "Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model", Information Systems Research, 15(4), 2004, pp. 336-355.

[13] Laufer, R.S., and Wolfe, M., "Privacy as a concept and a social issue: A multidimensional developmental theory", Journal of Social Issues, 33(3), 1977, pp. 22-42.

[14] Hong, W., Chan, F.K.Y., and Thong, J.Y.L., "Drivers and inhibitors of internet privacy concern: A multidimensional development theory perspective", Journal of Business Ethics, 2019, pp. 1-26.

[15] Myers, M.D., Qualitative research in business and management, Sage Publications Limited, 3rd, London, 2019.

[16] Patton, M.Q., Qualitative evaluation and research methods, SAGE Publications, Thousand Oaks, CA, 1990.

[17] Myers, M.D., and Newman, M., "The qualitative interview in IS research: Examining the craft", Information and organization, 17(1), 2007, pp. 2-26.

[18] Marshall, B., Cardon, P., Poddar, A., and Fontenot, R., "Does sample size matter in qualitative research?: A review of qualitative interviews in IS research", Journal of Computer Information Systems, 54(1), 2013, pp. 11-22.

[19] Braun, V., and Clarke, V., "Using thematic analysis in psychology", Qualitative research in psychology, 3(2), 2006, pp. 77-101.

[20] Becker, M., "Understanding users' health information privacy concerns for health wearables", 51st Hawaii International Conference on System Sciences, 2018, pp. 3261-3270.

[21] Mettler, T., and Wulf, J., "Physiolytics at the workplace: Affordances and constraints of wearables use from an employee's perspective", Information Systems Journal, 29(1), 2019, pp. 245-273.

[22] Kehr, F., Kowatsch, T., Wentzel, D., and Fleisch, E., "Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus", Information Systems Journal, 25(6), 2015, pp. 607-635.

[23] Maslow, A.H., "A theory of human motivation", Psychological review, 50(4), 1943, pp. 370-396.

[24] Ayyagari, R., Grover, V., and Purvis, R., "Technostress: Technological antecedents and implications", MIS Quarterly, 35(4), 2011, pp. 831-858.

[25] Brod, C., Technostress: The human cost of the computer revolution, Addison Wesley Publishing Company, Reading, MA, 1984.

[26] Miller, C., and Stuart Wells, F., "Balancing security and privacy in the digital workplace", Journal of Change Management, 7(3-4), 2007, pp. 315-328.