

A Synthesized Perspective on Privacy and Transparency in the Digital Workplace

Maren Gierlich-Joas
Munich School of Management
LMU Munich
gierlich@lmu.de

Mena Angela Teebken
Munich School of Management
LMU Munich
teebken@lmu.de

Thomas Hess
Munich School of Management
LMU Munich
thess@lmu.de

Abstract

The pandemic crisis has made the digitalization of workplaces imperative for many organizations. Besides reorganizing work, rapid advances in technologies also enhance organizational efficiency and enable remote work. Having to work completely digitally imposes unprecedented transparency on employees. A major consequence of the transparent workplace is the emergence of employees' privacy concerns. Even though the concepts of transparency and privacy are closely related, there is a research gap regarding the relationship between the two. Based on a conceptual approach and a systematic literature review, we postulate a synthesis of transparency and privacy in the digital workplace, and outline directions for future research. We discuss what makes the relationship between the two constructs double-edged by introducing the privacy-transparency paradox. This study therefore adds to the literature on privacy and transparency in the digital workplace and forms the basis for further studies.

1. Introduction

Organizations increasingly find themselves in flexible and rapidly changing environments where they are greatly exposed to digitalization [1, 2]. Consequently, driven by digitalization and remote working modes in times of a pandemic, the nature of work has changed fundamentally [2, 3]. Today, the use of novel technologies, agile ways of working, and the adjusting role of leadership characterize digital workplaces [4].

As a trigger and enabler of digital workplaces, workplace technologies have developed significantly. They are no longer limited to discrete office applications, but also cover integrated SMAC (social, mobile, analytics, and cloud) technologies [2, 4]. Furthermore, they enhance collaboration, communication and decision making at work. At the same time, these technologies automatically generate,

collect, store, and analyze employee data [2]. Following the paradigm “the more, the better,” organizations rely heavily on data as a foundation for digital products and services [5].

However, for those individuals who reveal personal information, the processing of their data can have benefits and risks. The availability of data leads to increasing levels of organizational transparency [6, 7]. Transparency therefore refers to the disclosure of information to different stakeholders, which is mostly enforced at work [7]. Correspondingly, privacy relates to individuals' ability to control the acquisition and revelation of their personal information [8]. On the one hand, transparency can be a mutual learning opportunity for employees, for teams an efficient way of working, and an enabler of trust in the entire organization [6, 7]. On the other hand, transparency can lead to strict supervision, which potentially leads to employees having privacy concerns [9, 10]. These privacy concerns relate to employees' concerns about what happens to their personal information revealed through the use of digital solutions at the workplace [9]. If privacy concerns are not thoroughly addressed, employees may fear being monitored or the information could overwhelm them [10, 11]. Therefore, transparency needs to be implemented strategically, allowing the benefits of transparency to outweigh the privacy concerns. We observe a close interaction, a trade-off, between transparency and privacy's core concepts.

Researchers often rely on an understanding of privacy from the consumer perspective when attempting to understand privacy concerns on the job [9]. However, since privacy settings at the workplace are characterized by their enforced nature, the subordinate relationship between employees and employers, and the types of data handled [9], insights from the consumer privacy context are difficult to transfer. We observe a lack of understanding, as “[t]o date, the transparency and privacy literature have talked past each other” (p. 219) [7].

Recent studies interpret the relationship between privacy and transparency as a one-way street. However, we believe that transparency can facilitate the overcoming of privacy concerns in the same way that it triggers them. In our understanding, privacy and transparency are two sides of the same coin. We therefore aim to close the gap between the concepts by investigating the research question:

How are privacy and transparency in the digital workplace related?

To address the research question, we follow a conceptual approach that the recommendations by Hirschheim [12] and Jaakkola [13] guide. The paper is therefore structured as follows: First, we reflect on the theoretical understanding of privacy and transparency. Next, we make use of a structured literature review on the relationship between both the concepts on which to base our claims (section 3). We present a conceptual model, guided by the multidimensional development theory (MDT), and specify the interaction between both the concepts in section 4. Next, the observed privacy-transparency paradox is discussed, which details the linkages between the constructs (section 5). Finally, we outline a research agenda in section 6, and summarize the findings in section 7.

The work contributes to an understanding of the challenges in the digital workplace, providing three-fold findings. First, our conceptual model shows how transparency can be a driver for privacy concerns, but also a solution for overcoming them. Second, we introduce the privacy-transparency paradox as a novel paradox. Third, the research agenda encourages further research.

2. Underlying concepts

Digital workplaces are becoming increasingly flexible, collaborative, and transparent, which entails both risks and benefits. We outline the literature's understanding of transparency and privacy concepts in the following, before investigating their combined occurrence and relationship in the workplace context.

2.1. Transparency in the workplace

The spread of workplace technologies leads to increasing levels of transparency inside companies [10]. The term "transparency" has different connotations: Some studies interpret transparency in a neutral way as "process visibility" or "information disclosure," while others define it as "monitoring" or "surveillance" [7]. The first definitions highlight transparency's benefits, whereas the latter emphasize threats resulting from increasing transparency.

Regarding the benefits, transparency facilitates organizational learning, communication, and collaboration [10, 14]. If data are visible, employees can work in self-determined ways and desirable behaviors are promoted [6, 7]. However, in terms of the risks, transparency is often implemented in one-directional, direct ways, allowing managers to oversee employees, but allowing employees limited insights. This type of direct transparency can lead to employee privacy concerns [9], a loss of motivation [15], increased worker stress [11], and negative impacts on employees' well-being [16]. Besides these empirical findings, we find theoretical arguments, like the privacy calculus, which highlight information disclosure's trade-off [17].

To prevent direct transparency having negative consequences, prior studies introduced inverse transparency [6]. Similar to the "downward transparency" concept, which aims to allow employees to oversee their managers' behavior [18], inverse transparency is implemented in a two-directional way [6]. The latter makes information flows visible to employees and facilitates their data sovereignty, thereby democratizing control. Inverse transparency can enable novel leadership approaches [19]. If the controller's intentions are transparent, this helps to reduce privacy concerns [20]. As a counterpart to direct transparency, we regard inverse transparency as meta-transparency in the sense of making transparency transparent [7]. Although inverse transparency might have shortfalls, it, unlike direct transparency, mainly addresses its positive outcomes.

2.2. Privacy in the workplace

The digitalization of the workplace has potential risks for employees, namely privacy concerns. Privacy literature differentiates between physical and information privacy as two distinct forms of an individual's privacy [8]. While the former describes physical access to an individual, the latter focuses on an individual's personal information. Information privacy relates to individuals' desire to control data about themselves and to influence their dissemination [21]. How individuals perceive privacy can differ, depending on various factors, such as demographics or personalities [8]. If the perceived privacy level is experienced as negative, the privacy concerns concept is investigated as a proxy for information privacy [8]. Privacy concerns emerge due to the growing collection, processing, usage, and resulting loss of control over personal information [8, 17].

The investigation of privacy and corresponding proxies to measure information privacy is context-dependent [8]. The literature indicates that when

individuals interact as employees, their perceptions of privacy in the job context differ from their perceptions in other contexts [22]. For instance, individuals at work have reduced control over their personal information, and experience a lack of freedom of choice regarding revealing this information in the first place [23]. Resulting from the need to investigate privacy as being distinct from an employee perspective, privacy research dedicated to workplace contexts is on the rise [9, 10]. Nonetheless, an integrative perspective of transparency is still lacking, leading to the emergence of workplace privacy concerns and a lacking understanding of how organizations can mitigate such concerns.

3. Structured literature synthesis

Prior literature has a common understanding of why privacy and transparency are considered trade-offs. Owing to their contextual nature, research findings on the relationship between transparency and privacy in general contexts cannot be seamlessly transferred to the work context. We therefore aim to deepen these initial insights.

We conducted a systematic literature review to create claims to build our further grounds and warrants on [12]. Following the guidelines by Paré et al. [24] for achieving transparency and systematicity during the review process, we focused on the eight journals comprising the AIS Senior Scholars' Basket. To take more recent publications on the pandemic into account, we also searched for contributions to the IS conferences ICIS, ECIS, PACIS, AMCIS, and HICSS from between August 2020 and August 2021. The search terms “Transparency AND Privacy AND Workplace” were applied to the full texts. The initial search yielded 124 papers, whose relevance for the research question we then assessed carefully. Contributions solely applying a customer perspective on transparency and privacy, or representing track introductions, were excluded from the analysis. The final sample consists of 28 papers (see Table 1).

Relationship	Sources
Transparency as a driver of privacy concerns	[9], [25], [26], [27], [28], [29], [30], [31], [32], [33], [34], [35], [36], , [37], [38], [39], [40], [41], [42], [43], [44], [45]
Transparency as a solution for privacy concerns	[26], [33], [38], [42], [44], [46], [47], [48], [49], [50]

Table 1. Literature on transparency and privacy in the workplace

We identified an increasing awareness of the topic, since only one contribution was from before 2013. Moreover, six journal contributions and most studies of the selected conferences address special calls relating to the COVID-19 pandemic. When analyzing the selected contributions, we investigated the outlined relationship between the privacy and transparency concepts. The two core dimensions, “transparency as a driver of privacy concerns” and “transparency as a solution to privacy concerns,” were distinguished inductively.

Most contributions can be assigned to the first dimension. In this cluster, we identify a group of papers that generally investigate the transparency’s impact on privacy concerns from a conceptual point of view. These contributions describe how organizations find themselves going “beyond the panopticon metaphor” when mobile IS establish novel control modes (p. 543) [31]. Prior works define this development as “surveillance capitalism” (p. 75) [36] that threatens individuals’ privacy. The COVID-19 crisis accelerates these trends, since remote work becomes the new normal, and workplace technologies become more important [9, 32, 35].

The second group in this first dimension applies a technology-centric view to investigate specific technologies’ impact on privacy concerns in the context of organizations. In this regard, the use of big data applications [29] and AI-based tools at work [25] could have severe negative impacts on organizational privacy. In addition, cognitive computer systems are mostly perceived as surveillance mechanisms [44]. Prior contributions highlight the existence of a privacy paradox in the workplace, since increasing privacy concerns mean information is increasingly shared with service robots [41]. There might be positive mechanisms for dealing with algorithmic control, although privacy concerns often arise and employees aim to distance themselves from their manager [40]. Moreover, communication and collaboration tools, like Yammer and Chatter [27], lead to increased levels of direct transparency and are often perceived as management surveillance tools [30]. Similarly, tracing tools for e-mails [37], digital productivity assistances [39] or personalized assistance systems [46] cause privacy concerns at the workplace. When employees work remotely, online recordings can specifically unsettle them [51]. Lastly, quantified self-practices track physical data [28]. These wearables are considered tools that facilitate monitoring, highlighting the downside of transparency [34]. Similarly, algorithms that track drivers’ ridesharing are perceived critically in terms of privacy [45]. Such digital platforms drive panoptic forms of surveillance [43].

In contrast, the second dimension represents “transparency as a solution for privacy concerns.” Papers in this category highlight opportunities to overcome the challenges of transparency, using transparency in positive ways. According to Markus, data-enabled transparency can either lead to transformation or to manipulation in organizations and is a double-edged sword [33]. For transparency to have a positive impact on privacy concerns, data should be exchanged on a team level. When the overall transparency level has increased, for example, in an enterprise social media tool, data should be exchanged for idea generation [49]. Sharing data between employees, for example, via groupware systems, helps reduce privacy concerns, although it might increase the complexity [26]. On a platform level, concealing information could establish trust between different stakeholders [48]. For example, the privacy concerns of employees working for a crowdsourcing platform could be decreased if their information is shared [47]. Analogously, some types of privacy nudges can help increase transparency [38]. Moreover, if AI is used in the recruitment process, providing transparency and offering bi-directional transparency can be a chance to reduce the applicants’ privacy concerns [50].

In summary, we find diverse views on the relationship between privacy and transparency in the workplace. Some stress the paradoxical tensions that digital technologies bring to the workplace [41, 42]. However, all contributions have their one-directional understanding of the relationship between the transparency and privacy concepts in common: Transparency is seen as either a threat to privacy or as an opportunity to decrease privacy concerns.

4. A conceptual model of the connection between privacy and transparency

Having stressed the research gap in the structured literature review, we now conduct a theory synthesis. Initially, we decompose the information privacy concept into its different layers, following the multidimensional development theory (MDT) explained in the next section. Thereafter, we integrate the supplemental relationship between direct and inverse transparency into a novel theoretical view in a conceptual model and derive a research agenda.

4.1. Multidimensional development theory as the underlying theoretical foundation

As suggested by Hirschheim [12], we use a framework as a theoretical lens to structure the conceptual model’s deviation. The extant literature

uses various theories to explain the observed phenomena of privacy issues [52, 53]. However, the majority of these theories are based on the privacy calculus concept, which explains how individuals weigh the benefits and risks of revealing personal information in exchange for the benefits of disclosing information [54]. In contrast, the MDT by Laufer and Wolfe [55] does not rely on privacy calculus mechanisms and describes how individuals’ concerns for privacy are the result of their environment, interpersonal interaction, and individual experiences. On a personal dimension, privacy concerns emerge over time as a result of self-development processes focusing on autonomy. The interpersonal interaction dimension explains how an individual’s privacy concerns emerge from the dyadic relationship between an individual and others based on the exchange of information. The environmental dimension describes how individuals develop privacy concerns as a result of cultural, social, and physical settings’ impacts. [55]

The MDT was previously used in various contexts to describe phenomena pertaining to information privacy issues [54]. In the following, the three-dimensional angle on information privacy is used to classify the drivers that enforce privacy concerns by direct transparency and the approaches that mitigate privacy concerns by inverse transparency.

4.2. The conceptual model

In Figure 1, we show the conceptual model in respect of the connection between privacy and transparency in the workplace along the aforementioned MDT’s dimensions. The circles represent the three-layered personal, interpersonal, and environmental spheres of privacy. The arrows highlight the data flow of the traditional understanding of enforced, direct transparency as a trigger for privacy concerns. The dotted arrows show the inverse transparency view as a solution to overcome privacy concerns (see numbers 1-5).

Personal information: The model’s starting point is the revelation, circulation, and diffusion of information on the employee through the use of digital tools at work. Thereby, personal information can be collected explicitly or implicitly in an intentional or unintentional manner. For instance, employees reveal personal information, such as their address, date of birth or banking details, when signing their workplace contract. This revelation of data can be referred to as explicit and intentional. At the same time, employees implicitly and unintentionally reveal their personal information. For example, digital tools can automatically collect sensitive user data, such as GPS locations or IP addresses. On the one hand, implicitly

collected information can be performance-related and, for instance, used to assess employees' productivity. On the other hand, this information can also cross the boundaries to the employee's personal sphere, for instance, when communicating via video from the home office. The transition from working at the office to doing so remotely, and digital working modes, increase the blurring of contextual boundaries between employees' work and private identity, adding potential sources of personal information to be collected. The term "personal information" therefore covers various types of information that the digital workplace reveals and which can be traced back to an individual employee.

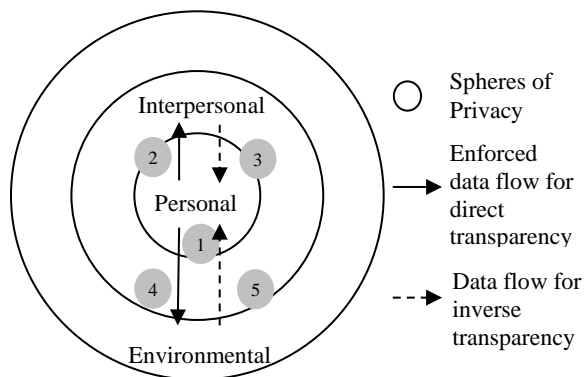


Figure 1: Three-dimensional conceptual model of the connection between privacy and transparency

Contextualization in the digital workplace: The peculiarity of the perspective on privacy and transparency from the employees' viewpoint is the benefit appraisal process in an underlying cost-benefit analysis. In a workplace context, employees do not get to weigh the benefits and risks of information disclosure. Conversely, in a job context, the revealing of personal information is enforced. Owing to an employee's dependence on an employer and to the subordinate relationship between the two, in the workplace context, control over personal information is shifting from the individual to the organization's direction. In addition, in a job setting, digital tools are not designed to provide personal benefits for disclosing data, but are an essential part of the digital workplace, for example, to collaborate or communicate [56]. Therefore, in a work context, there is no benefit appraisal as in the consumer context. This leads to inverse transparency having a different role in the workplace context than in the consumer context [6].

In the following paragraphs, we outline the two concepts' interaction on each dimension by describing direct transparency's effects and the perception of inverse transparency, whereas the numbers in brackets in the model indicate the position.

Personal sphere: On the personal level, several factors, such as individual characteristics, demographics, attitude or trust can drive an employee's privacy valuation (1). In a workplace context, direct transparency can lead to employees being transparent in all situations where the digital tool usage is essential. This can affect both primary workplaces and remote ones. Since employees' personal traits and internal beliefs drive these privacy concerns, there are no major levers for ex-ante preventing these concerns. However, companies could apply certain measures to deal with concerns related to individuals' beliefs ex-post, like matching an individual's privacy preferences with suitable job environments at the firm.

Interpersonal sphere: On the interpersonal level, privacy concerns arise as a result of the interaction between an employee and other stakeholders. These stakeholders can be internal, such as colleagues or supervisors, or external, such as customers.

The usage of digital solutions imposes direct transparency of an employee's personal information, which leads to an exchange of information with other stakeholders (2). This can occur through various job practices that enable communicating about and collaborating on operative tasks. In this dimension, transparency is imposed on employees since they do not always get to decide what information to share with whom. In this scenario, employees have no chance to adjust their privacy settings, nor can they understand or control the use of their data. On an interpersonal dimension, inverse transparency measures aim to reduce privacy concerns (3). Such measures include, for instance, privacy-by-design practices or implementations such as privacy dashboards. If systems follow privacy-by-design principles, individuals can see the flow of personal information and have opt-in options regarding with whom to share their data. They can therefore manage their data and control their usage. However, inverse transparency goes a step further, as data can conversely be shared inside the company. If teams have access to their data, they can work in self-organized ways, which enhances trust. If managers share their insights and transparently demonstrate how they use data for decision-making, privacy concerns can be reduced.

Environmental sphere: Lastly, in the environmental dimension, cultural, social, and physical settings, including the regulatory and technological framework, form the privacy perception. Environmental aspects can impose direct transparency regarding individuals' environment, thereby creating concerns for privacy (4). Sensitivity about privacy differs across nations and cultures [8]. In terms of the

physical environment, the use of personal information and communication technologies plays a crucial role. If employees are expected to use their private devices when working remotely or to use a device for both private and professional purposes, this can undermine their privacy. The regulatory framework, which aims to protect an employee’s privacy, does not necessarily include novel technological advances once they are implemented [23]. On the environmental level, inverse transparency can help ease privacy concerns (5). While cultural drivers are difficult to change, the physical environment can be designed in privacy-friendly ways. There is a need for clear boundaries between private and professional device usage and a transparent understanding of whether an employee is on private time or working. A cohesive regulatory framework protects employee privacy adequately and an assessment of transparency requires a continuous reflection of technological advances.

Overall, our conceptual model displays direct transparency and inverse transparency as two opposing, but yet complementary, concepts that each have distinct impacts on the three privacy spheres.

5. The privacy-transparency paradox

The theory synthesis on privacy and transparency in the workplace in section 4 provides insights into the two-directional relationship between the two. Privacy and transparency can be considered not yet adequately matched problems and solutions. Distinguishing between direct transparency on the one side and inverse transparency on the other side sheds light on their two-directional impact on perceived privacy. On the one hand, direct transparency diminishes actual information privacy. The imposed transparency leads to privacy concerns, which serve as a proxy for information privacy [8]. On the other hand, when inverse transparency is implemented in favor of employees, this reduces their perceived lack of privacy [6]. While inverse transparency helps employees to trust their companies and mitigate their privacy concerns, it cannot provide actual information privacy. Direct transparency and inverse transparency do not, therefore, operate on the same level. Conversely, the former is directed at actual information privacy, while the latter is directed at perceived privacy concerns (see Figure 2). Based on this understanding, we frame the ambiguity between our model’s two core concepts as the “privacy-transparency paradox.”

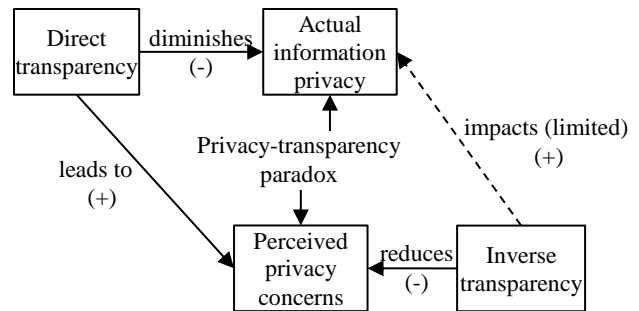


Figure 2. The privacy-transparency paradox

The paradoxes theory is used as a meta-theory to explain organizational tensions and how they can be overcome [57]. Accordingly, scholars have used it to explore the relationships between two opposing elements [57]. Paradoxes describe competing demands, goal conflicts or wicked problems. The literature distinguishes between various paradoxes to describe these problems, their origin, and their handling [58]. Prominent examples are the privacy paradox [59] and the transparency paradox [60]. We build on these established paradoxes, which are closely related to the study at hand, when introducing the privacy-transparency paradox as a novel type. For a comparison of established and new paradoxes, we follow the opposing elements’ dimensions, perceived tensions, scope, response to contradiction, and outcome [58] to compare the models and underline the novelty of our idea (see Table 2).

Starting with the privacy paradox, the opposing elements are the intention to disclose private information and the actual disclosure behavior. These tensions are predominately observed in the consumer context. Concerning handling the contradiction, authors often apply the “either-or-approach” [58]. This implies that one activity has to be selected from multiple, incompatible ones. Consequently, defensive mechanisms are applied that focus on coping with the paradox instead of solving it, with the outcomes being unintended and unanticipated actions. In this case, data are shared, although this was not desired [59].

In respect of the transparency paradox, performance under observation and under privacy is the opposing force. Counterintuitively, observability may reduce performance, whereas, creating zones of privacy may increase performance in the workplace context. Management often follows a “both-and-approach” and tries to find a balance between the elements when handling the paradox [58]. Consequently, they endeavor to meet the competing demands of organizational transparency and privacy by trying to neutralize the tension. This can, however, result in constraining actions [7, 60].

Building on these paradoxes, we derive the privacy-transparency paradox. Hereby, the two forms of transparency have opposing relationships with privacy-related constructs. While counterintuitive at first glance, when this privacy-transparency paradox distinguishes between different types of transparency, direct and inverse, with their own *raison d'être* and different directions of effectiveness, this dissolves the paradox. While direct transparency affects actual information privacy, inverse transparency addresses privacy at the level of perceived privacy concerns. Owing to the enforced type of transparency, the digital workplace is the paradox's scope. In contrast to the other paradoxes, the handling of the paradox is rather solution oriented, since it follows a "more-than-approach" [58]. This means that we use the dynamic interplay between the opposites to provide a novel perspective. By reframing and connecting established concepts in the digital workplace, new opportunities, for example, new ways of leadership, become feasible. This leads to an opening up in the organization, which challenges power relations between its managers and employees. Unlike in prior paradoxes, the goal is not to "tame" the paradox by either eliminating it or working around it. Instead, the privacy-transparency paradox provides a novel way of reframing organizational tensions in the context of privacy and transparency.

	Privacy Paradox	Transparency Paradox	Privacy-transparency paradox
Opposing elements	Intention to disclose and actual disclosure	Performance under observation and in privacy	Impact of direct and inverse transparency on privacy
Perceived tensions	Intentions to disclose information do not match the actual sharing behavior of that information	Observability reduces performance, but, conversely, creating zones of privacy could increase performance	Direct transparency reduces actual information privacy, inverse transparency reduces perceived privacy concerns
Scope	Consumer	Workplace	Workplace
Response to contradiction	Either-or-approach: defensive mechanism	Both-and-approach: integration and balance	More-than-approach: reframing & connection
Outcome	Unintended actions	Enabling & constraining	Opening up
Source	[59]	[7, 60]	This study

Table 2. Comparison of research field paradoxes

6. Research Agenda

Based on the conceptual model and the outlined privacy-transparency paradox, we suggest avenues for further research (see Table 3). With regard to the personal sphere, employees' valuation of privacy needs to be understood. The investigation of the determinants of privacy concerns can be embedded in APCO (Antecedents-Privacy Concerns-Outcome) macro models for a cohesive investigation of privacy concerns as a dependent or independent variable [8], especially in combination with different forms of transparency as an antecedent. Future studies need to define the employee's touchpoints with digital solutions, and map them to represent the employee's journey, which is similar to the customer journeys concept. On this basis, one can derive how direct transparency can lead to privacy concerns, and how individual privacy preferences can be met in the workplace.

In respect of the interpersonal sphere, researchers need to investigate whether the digital workplace actually allows information privacy. Based on the employee journey from the personal dimension, it is essential to identify privacy-threatening stakeholders from an internal and external point of view. Furthermore, practices in the employees' line of interaction need to be identified in order to define levers for privacy and transparency practices at work. Following the theory of multilevel information privacy management [61], future research should also explore the topic from a group perspective, where stakeholders co-own information.

In respect of the environmental sphere, research needs to investigate who is responsible for employees' privacy on a normative level. This includes assessing whether digital solution providers should be held responsible for incorporating privacy-by-design measures or the measures organizations can take to reduce their employees' privacy concerns. Furthermore, companies need to evaluate the value of privacy for their business models. On a descriptive level, future research should investigate environmental factors' impact on privacy concerns.

Regarding the privacy-transparency paradox, future research needs to investigate how the tradeoff plays out in practice, for example, how employees perceive the connection between direct and inverse transparency. We encourage researchers to investigate how the degree of direct and inverse transparency should be imposed on employees. Following this, future research should investigate the limits of privacy in the context of the digital workplace.

Research dimension	Exemplary research questions
Personal sphere	<ul style="list-style-type: none"> • What are employees' privacy perceptions, beliefs, and threats? • What are the determinants of privacy concerns in the workplace? • What does an employee's journey look like in terms of the data touchpoints? • How can the workplace be adapted for individual privacy preferences?
Interpersonal sphere	<ul style="list-style-type: none"> • How can privacy at the digital workplace be enhanced given the different stakeholders? • How can data owned by groups be managed?
Environmental sphere	<ul style="list-style-type: none"> • Who is responsible for privacy at the workplace? • What value does workplace privacy have? • How can companies reduce their employees' privacy concerns? • What environmental factors influence privacy concerns at work?
Privacy-transparency paradox	<ul style="list-style-type: none"> • How can inverse transparency be established in practice? • What is the right level of direct and inverse transparency?

Table 3. Research agenda for privacy and transparency at the workplace

7. Conclusion

Even though the workplace is becoming increasingly digital, there is a lacking understanding of the resulting challenges. A central problem is balancing trust and surveillance in digital work. In this setting, transparency and privacy are two sides of the same coin. However, both concepts have only been investigated in fragmented ways, therefore missing a synthetic view that connects the learnings from both fields. We address and extend existing research by applying a conceptual approach to the research question: *How are privacy and transparency in the digital workplace related?* In our three-fold approach, we develop a conceptual model, introduce the privacy-transparency paradox to highlight their ambivalent relationship, and, finally, derive an agenda for future research. We therefore make these contributions:

First, we contribute to the understanding of the digitalization of work. At digital workplaces, trust and surveillance mechanisms are strongly interwoven, challenging both managers and employees. Considering transparency and privacy at work sheds light on digital work's conceptual design.

Second, the study provides a basis by uncovering privacy and transparency concepts in the workplace in

nuanced ways. So far, privacy research has lacked the workplace perspective, and rather focused on consumer settings. Transparency is predominately defined as direct, one-directional transparency, which lacks an interpretation of inverse, two-directional transparency.

Third, we achieve conceptual integration across the existing research streams and link both previously unconnected concepts. The MDT lens provides a helpful theoretical foundation for deriving a higher-order perspective of the phenomenon. Consequently, the conceptual model helps us understand the "big picture" of how privacy and transparency are related.

Fourth, by illustrating a research agenda that relates to the MDT dimensions and covers normative and descriptive approaches, we hope to encourage scholars to conduct related studies. We regard our work as a stepping-stone that calls for further investigation.

Lastly, the paper adds to the literature on paradoxes by shedding light on the "wicked" relationship between two concepts. The privacy-transparency paradox enhances prior research defining a privacy-paradox [59] or a transparency-paradox [60] without connecting both.

Due to its nature, the study predominately holds theoretical contributions. However, the trade-off between privacy and transparency is highly relevant for practitioners, especially when remote work is a must. For companies, questions on how to ensure organizational privacy while still being able to use data for digital innovation, collaboration and new ways of work, are pressing challenges. Our understanding of the relationship between privacy and transparency points to measures for how these challenges can be overcome. Being transparent about privacy settings and sharing data across employees and teams can reduce privacy concerns, making inverse transparency favorable. Inverse transparency should be favored instead of direct transparency. Still, these preliminary findings need to be transferred into guidelines that were not in scope.

Though conducted thoroughly, our study does not come without limitations. The conceptual interpretation of both core concepts is impacted by the perception of both authors and is not necessarily exhaustive. The conceptual model and the privacy-transparency-paradox are motivated by the workplace context but can be transferred to the consumer context. If applied to the consumer context, the imposed nature of direct transparency is weakened and the role of inverse transparency as a foremost measure to encounter imposed data revelation will decrease. In terms of methodology, a conceptual approach differs from empirical investigations. This implies that the

derived model is not grounded on empirical observations, could not yet be tested and might come with biases or shortfalls. To add explanatory power to our argumentation, we based our claims on a structured literature review and reflected our thoughts in the light of the MDT. Still, empirical investigations on the relationship between privacy and transparency in the workplace are important. Thus, concerning these limitations, we encourage scholars to follow our outlined agenda for research by addressing research questions along the three dimensions. As digital workplaces become the “new normal”, issues surrounding transparency and privacy require further attention. Novel digital solutions applied at work will continuously challenge the concept of privacy, making the two-sided interpretation of transparency even more essential.

8. References

- [1] Faraj, S., Renno, W., and Bhardwaj, A., "Unto the breach: What the COVID-19 pandemic exposes about digitalization", *Information and Organization*, 31(1), 2021, pp. 1-7.
- [2] Baptista, J., Stein, M.-K., Klein, S., Watson-Manheim, M.B., and Lee, J., "Digital work and organisational transformation: Emergent Digital/Human work configurations in modern organisations", *The Journal of Strategic Information Systems*, 29(2), 2020, pp. 1-10.
- [3] Scholz, T., *Big Data in Organizations and the Role of Human Resource Management*, Volker Stein, New York, 2017.
- [4] Jensen, T.B., and Stein, M.-K., "Designing a Digital Workplace: Introducing Complementary Smart Work Elements", *Journal of Financial Transformation*, 52, 2021, pp. 42-53.
- [5] Baskerville, R., Myers, M.D., and Yoo, Y., "Digital First: The Ontological Reversal and New Challenges for IS Digital First: The Ontological Reversal and New Challenges for IS Research", *MIS Quarterly*, 44(2), 2020, pp. 509-523.
- [6] Gierlich-Joas, M., Hess, T., and Neuburger, R., "More Self-Organization, More Control – Or Even Both? Inverse Transparency As A New Digital Leadership Concept", *Business Research*, 13, 2020, pp. 921–947.
- [7] Bernstein, E., "Making Transparency Transparent: The Evolution of Observation in Management Theory", *Academy of Management Annals*, 11(1), 2017, pp. 217-266.
- [8] Smith, H.J., Dinev, T., and Xu, H., "Information Privacy Research: An Interdisciplinary Review", *MIS Quarterly*, 35(4), 2011, pp. 989-1015.
- [9] Teebken, M., and Hess, T., "Privacy in a Digitized Workplace: Towards an Understanding of Employee Privacy Concerns", *HICSS*, 2021.
- [10] Bhave, D.P., Teo, L.H., and Dalal, R.S., "Privacy at Work: A Review and a Research Agenda for a Contested Terrain", *Journal of Management*, 46(1), 2020, pp. 127-164.
- [11] Tams, S., Ahuja, M., Thatcher, J., and Grover, V., "Worker stress in the age of mobile technology: The combined effects of perceived interruption overload and worker control", *The Journal of Strategic Information Systems*, 29(1), 2020, pp. 1-10.
- [12] Hirschheim, R., "Some Guidelines for the Critical Reviewing of Conceptual Papers", *Journal of the Association for Information Systems*, 9(8), 2008, pp. 432-441.
- [13] Jaakkola, E., "Designing conceptual articles: four approaches", *AMS Review*, 10(2020), pp. 18-26.
- [14] Bernstein, E., "The Transparency Paradox: A Role for Privacy in Organizational Learning and Operational Control", *Administrative Science Quarterly*, 57(2), 2012, pp. 181-216.
- [15] Valentinov, V., Verschragenen, G., and Van Assche, K., "The limits of transparency: A systems theory view", *Systems Research and Behavioral Science*, 36, 2019, pp. 289-300.
- [16] Alder, G.S., "Employee reactions to electronic performance monitoring: A consequence of organizational culture", *The Journal of High Technology Management Research*, 12(2), 2001, pp. 323-342.
- [17] Dinev, T., and Hart, P., "An extended privacy calculus model for E-commerce transactions", *Information Systems Research*, 17(1), 2006, pp. 61-80.
- [18] Heald, D., "Varieties of transparency", in (Hood, C., and Heald, D., eds.): *Transparency: The key to better governance?*, Oxford University Press, 2006, pp. 25-43.
- [19] Gierlich-Joas, M., "Identifying and Overcoming Future Challenges in Leadership: The Role of IS in Facilitating Empowerment", *Wirtschaftsinformatik*, 2021
- [20] Oulasvirta, A., Suomalainen, T., Hamari, J., Lampinen, A., and Karvonen, K., "Transparency of Intentions Decreases Privacy Concerns in Ubiquitous Surveillance", *Cyberpsychology, Behaviour, and Social Networking*, 17(10), 2014, pp. 1-6.
- [21] 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.
- [22] Nord, G.D., Mccubbins, T.F., and Nord, J.H., "E-monitoring in the workplace: Privacy, legislation, and surveillance software", *Communications of the ACM*, 49(8), 2006, pp. 72-77.
- [23] Teebken, M., "What Makes Workplace Privacy Special? An Investigation of Determinants of Privacy Concerns in the Digital Workplace", *AMCIS*, 2021.
- [24] Paré, G., Tate, M., Johnstone, D., and Kitsiou, S., "Contextualizing the twin concepts of systematicity and transparency in information systems literature reviews", *European Journal of Information Systems*, 25, 2016, pp. 493–508.
- [25] Benbya, H., Pachidi, S., and Jarvenpaa, S.L., "Artificial Intelligence in Organizations: Implications for Information Systems Research", *Journal of the Association for Information Systems*, 22(2), 2021, pp. 281-303.
- [26] Bordetsky, A., and Mark, G., "Memory-based feedback controls to support groupware coordination", *Information Systems Research*, 11(4), 2000, pp. 366-385.
- [27] Choudrie, J., and Zamani, E.D., "Understanding individual user resistance and workarounds of enterprise social networks: the case of Service Ltd", *Journal of Information Technology*, 31(2), 2016, pp. 130-151.

- [28] De Moya, J.F., and Pallud, J., "From panopticon to heautopticon: A new form of surveillance introduced by quantified-self practices", *Information Systems Journal*, 30(6), 2020, pp. 940-976.
- [29] Gunther, W.A., Mehrizi, M.H.R., Huysman, M., and Feldberg, F., "Debating big data: A literature review on realizing value from big data", *Journal of Strategic Information Systems*, 26(3), 2017, pp. 191-209.
- [30] Koch, H., Leidner, D.E., and Gonzalez, E.S., "Digitally enabling social networks: resolving IT-culture conflict", *Information Systems Journal*, 23(6), 2013, pp. 501-523.
- [31] Leclercq-Vandelannoitte, A., Isaac, H., and Kalika, M., "Mobile information systems and organisational control: beyond the panopticon metaphor?", *European Journal of Information Systems*, 23(5), 2017, pp. 543-557.
- [32] Marabelli, M., Vaast, E., and Li, J.L., "Preventing the digital scars of COVID-19", *European Journal of Information Systems*, 30(2), 2021, pp. 176-192.
- [33] Markus, M.L., "Datification, Organizational Strategy, and IS Research: What's the Score?", *Journal of Strategic Information Systems*, 26(3), 2017, pp. 233-241.
- [34] Mettler, T., and Wulf, J., "Physiolitics at the workplace: Affordances and constraints of wearables use from an employee's perspective", *Information Systems Journal*, 29(1), 2019, pp. 245-273.
- [35] Wang, B., Schlagwein, D., Cecez-Kecmanovic, D., and Cahalane, M.C., "Beyond the Factory Paradigm: Digital Nomadism and the Digital Future(s) of Knowledge Work Post-COVID-19", *Journal of the Association for Information Systems*, 21(6), 2020, pp. 1379-1401.
- [36] Zuboff, S., "Big other: surveillance capitalism and the prospects of an information civilization", *Journal of Information Technology*, 30(1), 2015, pp. 75-89.
- [37] Hüllmann, J.A., and Krebber, S., "Identifying Temporal Rhythms using Email Traces", *AMCIS*, 2020.
- [38] Barev, T.J., Schwede, M., and Janson, A., "The Dark Side of Privacy Nudging – An Experimental Study in the Context of a Digital Work Environment", *HICSS*, 2021.
- [39] Winikoff, M., Cranefield, J., Li, J., Richter, A., and Doyle, C., "The Advent of Digital Productivity Assistants: The Case of Microsoft MyAnalytics", *HICSS*, 2021.
- [40] Pregonzer, M., Remus, U., and Wiener, M., "Algorithms in the Driver's Seat: Explaining Workers' Reactions to Algorithmic Control", *ECIS*, 2021.
- [41] Stock-Homburg, R., and Hannig, M., "Is There a Privacy Paradox in the Workplace?", *ICIS*, 2020.
- [42] Schneider, S., and Kokshagina, O., "Digital Technologies in the Workplace: A Ne(s)t of Paradoxes", *ICIS*, 2020.
- [43] Chai, S.H., Nicholson, B., Scapens, R.W., and Yang, C., "Digital Platforms, Surveillance and Processes of Demoralization", *ICIS*, 2020.
- [44] Welck, M., Derdak, I.J., and Veit, D., "Understanding Individuals' Perceptions Regarding Cognitive Computing Systems", *ICIS*, 2020.
- [45] Jiang, J., Adam, M., and Benlian, A., "Algoactivistic Practices in Ridesharing - A Topic Modeling & Grounded Theory Approach", *ECIS*, 2021.
- [46] Voss, M., Hoebertz, M., Bosak, O., Mohsenzadeh, F., Schnebke, M., Poeppelbuss, J., and Eisenbeiss, M., "Privacy-Centered Design Principles for Employee-Determined Data Collection and Use in Personalized Assistance Systems", *AMCIS*, 2021.
- [47] Deng, X.F., Joshi, K.D., and Galliers, R.D., "The Duality of Empowerment and Marginalization in Microtask Crowdsourcing: Giving Voice to the Less Powerful through Value Sensitive Design", *MIS Quarterly*, 40(2), 2016, pp. 279-302.
- [48] Hong, S.J., Bauer, J.M., Lee, K., and Granados, N.F., "Drivers of Supplier Participation in Ride-Hailing Platforms", *Journal of Management Information Systems*, 37(3), 2020, pp. 602-630.
- [49] Van Osch, W., and Bulgurcu, B., "Idea Generation in Enterprise Social Media: Open versus Closed Groups and Their Network Structures", *Journal of Management Information Systems*, 37(4), 2020, pp. 904-932.
- [50] Hekkala, S., and Hekkala, R., "Integration of Artificial Intelligence into Recruiting Young Undergraduates: the Perceptions of 20–23-Year-Old Student", *HICSS*, 2021.
- [51] Cardon, O., Ma, H., Fleischmann, A.C., and Aritz, J., "Recorded Work Meetings and Algorithmic Tools: Anticipated Boundary Turbulence", *HICSS*, 2021.
- [52] Li, Y., "Theories in online information privacy research: A critical review and an integrated framework", *Decision Support Systems*, 54(1), 2012, pp. 471-481.
- [53] Kenny, G., and Connolly, R., "Drivers of Health Information Privacy Concern: A Comparison Study", *AMCIS*, 2016.
- [54] 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*, 168, 2021, pp. 539-564.
- [55] 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.
- [56] Attaran, M., Attaran, S., and Kirkland, D., "The need for digital workplace: increasing workforce productivity in the information age", *International Journal of Enterprise Information Systems*, 15(1), 2019, pp. 1-23.
- [57] Schad, J., and Bansal, P., "Seeing the Forest and the Trees: How a Systems Perspective Informs Paradox Research", *Journal of Management Studies*, 55(8), 2018, pp. 1490-1506.
- [58] Putnam, L.L., Fairhurst, G.T., and Banghart, S., "Contradictions, Dialectics, and Paradoxes in Organizations: A Constitutive Approach", *The Academy of Management Annals*, 10(1), 2016, pp. 65–171.
- [59] Norberg, P., Horne, D.R., and Horne, D.A., "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors", *The Journal of Consumer Affairs*, 41(1), 2007, pp. 100-126.
- [60] Bernstein, E., "The Transparency Paradox: A Role for Privacy in Organizational Learning and Operation Control", *Administrative Science Quarterly*, 57(2), 2012, pp. 181-216.
- [61] Bélanger, F., and James, T.L., "A Theory of Multilevel Information Privacy Management for the Digital Era", *Information Systems Research*, 31(2), 2020, pp. 510-536.