Grisold, Thomas; Seidel, Stefan; Heck, Markus; Berente, Nicholas

Digital Surveillance in Organizations

Business & Information Systems Engineering

Suggested Citation: Grisold, Thomas; Seidel, Stefan; Heck, Markus; Berente, Nicholas (2024) : Digital Surveillance in Organizations, Business & Information Systems Engineering, ISSN 1867-0202, Springer Fachmedien Wiesbaden, Wiesbaden, Vol. 66, Iss. 3, pp. 401-410, https://doi.org/10.1007/s12599-024-00866-7

Bus Inf Syst Eng 66(3):401–410 (2024)
https://doi.org/10.1007/s12599-024-00866-7

CATCHWORD

Digital Surveillance in Organizations

Thomas Grisold · Stefan Seidel · Markus Heck · Nicholas Berente

Accepted: 28 March 2024 / Published online: 27 June 2024

Keywords Digital surveillance · Digital trace data · Artificial intelligence · Control · Behavioral visibility

1 Introduction

The increasing digitalization and datafication of all aspects of our private and professional lives have led to widespread digital surveillance (e.g., Zorina et al. 2021). The roots of digital surveillance lie in the growing share of our everyday behavior that can be turned into quantifiable data objects, thus making it visible to and analyzable by others (Leonardi and Treem 2020). Recent research focuses attention on the implications of digital surveillance *in organizations*, as an increasingly large part of employee behavior is tracked and monitored as they use a variety of digital technologies to perform their work (Bernstein 2017; De Vaujany et al. 2021; Mettler 2023; Zorina et al. 2021). For instance, Gartner Inc. (2019) reports that in a survey of 239 large corporations, more than 50% use some type of non-traditional monitoring techniques, including the analysis of emails and social-media messages, or the collection of biometric data to determine how employees use their workspace (also see e.g., Ball 2021). Digital surveillance in organizations is tied to the assumption that scientific management can be embraced at new levels because the increasing amount of information also increases the means to monitor and improve efficiency and effectiveness (Bernstein 2017; Zorina et al. 2021).

Certainly, control and monitoring have been prevalent themes in the study of organizations for more than a century (Yates 1993). However, the ubiquitous nature of digital technologies, the associated data streams, and advances in the application of analytical software powered by artificial intelligence (AI), produce both a qualitatively and a quantitatively different situation. Organizations – and those who manage them – face entirely new possibilities for quantifying employees' behaviors and evaluating them in relation to organizational goals (Ball 2021). For example, organizations that capitalize on contemporary internet of things (IoT) technologies with sensors that allow for storing granular data streams of all sorts of activities, can use this data to assess and improve work performance, often in real time. For those who work in organizations, it is increasingly difficult – if not impossible – to be "invisible" (Leonardi and Treem 2020). Moreover, it becomes cheaper and cheaper to deploy digital surveillance initiatives (Ajunwa et al. 2017). The result is that the digital age brings "a wider economic imperative driving the expansion of digital surveillance in the workplace" (Spicer 2017).

The aim of this catchword article is to describe *digital surveillance in organizations* as a socio-technical phenomenon that is of interest to the information systems field. With digital surveillance in organizations, we refer to

Accepted after three revisions by Christine Legner.

T. Grisold
University of St. Gallen, Müller-Friedberg-Strasse 6/8,
9000 St Gallen, Switzerland
e-mail: thomas.grisold@unisg.ch

S. Seidel (✉)
University of Cologne, Pohligstraße 1, 50969 Cologne, Germany
e-mail: stefan.seidel@wiso.uni-koeln.de

M. Heck
SAP SE, Dietmar-Hopp-Allee 16, 69190 Walldorf, Germany
e-mail: markus.heck@sap.com

N. Berente
University of Notre Dame, Notre Dame, IN 46556, USA
e-mail: nberente@nd.edu

surveillance initiatives in organizational contexts that make use of digital traces and capitalize on digital technologies to provide insights into employees' behaviors and also act upon those insights. We conceptualize digital surveillance in organizations, discuss its various forms, and point to avenues for future research.

2 Digital Surveillance in Organizations

2.1 The Role of Information Technology in Surveillance

Surveillance has become an essential element of the functioning of modern organizations. Surveillance refers to an organization's attempt to purposefully and systematically perform close and constant supervision of the behaviors and characteristics of one or more employees, typically for the sake of controlling, influencing, or managing their behavior (e.g., Bernstein 2017). It involves the collection of information about activities, communications, and relationships between employees (Clarke 1988) and has been associated with establishing workers' compliance and conformity with organizational goals and values (Clarke 2019; Zorina et al. 2021).

Essentially, surveillance in organizations is about control and aims at driving productivity and efficiency. Surveillance in organizations is often likened to Foucault's (1977) version of the panopticon (Zuboff 1988). The panopticon describes a design of a prison with a central surveillance point that can observe every inmate. It is an apparatus of extensive control because the inmates never know when they are being observed, but they know that it could be any time. They internalize the control and act as the agents of their own control. Essentially, the mechanism through which the panopticon controls the inmates is self-discipline (Foucault 1977). This self-disciplining behavior is common for those who are under surveillance (Grey 1994). An important characteristic of surveillance in organizations is that employees develop the growing suspicion of being observed, so they subjugate themselves to the real or imaged expectations of those who are in power. Those who are being surveilled, then, may "reliably watch over themselves" (Boyne 2000, p. 299). Thus, surveillance goes beyond control: Whereas control is purposive and aims to motivate workers to perform in accordance with communicable organizational objectives (Clegg 1981), surveillance can be undirected in the sense that information is collected for general purposes with unclear consequences for employees (Ajunwa et al. 2017).

Information technology is associated with new means for deploying surveillance in organizations, and surveillance facilitated by information technologies is often associated with top-down, depersonalized control, where managers codify and automate work and work-related decisions, essentially deskilling and limiting the discretion of the workforce. For decades, however, research has shown that the effect of control-oriented information technologies is not simple. Although computerization can indeed involve automation and depersonalization, it can also result in the development of "intellective" skills and empowerment by providing information to the workforce and enhancing many elements of their work (i.e., "informatig," Zuboff 1988). Broad-scale control systems like enterprise resource planning (ERP) ratchet up control in the organization but can also empower the workforce by increasing visibility into organizational activities (Elmes et al. 2005). Further, implementing control technology is never easy. Employees can react to the introduction of the system through various forms of resistance, circumvention, gaming, and loose coupling (Berente et al. 2019). If the managers respond to attempts to circumvent the system with more control, this can result in cycles of resistance and circumvention that move further and further out of control (i.e., "drift," Ciborra 2000). Sometimes the availability of the control technologies can be used by workers to surveil and control the manager (Yates 1993) since many work-related behaviors, including those of managers, are now recorded and can be made available for various forms of analysis (e.g., Ball 2021; Leonardi and Treem 2020; Zickuhr 2021).

2.2 Features of *Digital* Surveillance in Organizations

Because tasks in organizations are increasingly performed with or enabled by digital technologies, employers can gain granular, high-frequency, and near real-time insights into employees' behavior (Zickuhr 2021). Digital technologies that use AI can identify patterns in this data and even take action on their own (Park 2021). Considering the far-reaching implications of these developments for employees and organizations, it is important to understand the dynamics and consequences of what we refer to as *digital surveillance* in organizations – that is, surveillance initiatives in work contexts that leverage digital traces of various sorts and capitalize on digital technologies to provide insights and also act upon those insights.

We can identify four key features of digital surveillance in organizations: a work context, digitalized behavior, watchers who monitor work-related behavior of those who are being watched, and digital processors to analyze traces of digitalized behavior.

2.2.1 Work Context

Digital surveillance in organizations occurs in work contexts in which one or more workers (inter)act to achieve certain organizational goals. These organizations can be for-profit organizations, governmental organizations, as well as non-governmental non-profit organizations. They can implement traditional forms of organizing with physical boundaries, such as in the case of manufacturing companies and call centers (Ball 2021), or can implement novel forms of organizing based on remote work that are typically associated with the gig-economy (Newlands 2021). Organizations may claim good intentions when they implement or increase digital surveillance, such as when they use a "rhetoric of safety," arguing that safety is enabled by more insights into workers' behavior (Rosenblat et al. 2014). Yet, the actual purpose is often to increase discipline and compliance (Bernstein 2017; De Vaujany et al. 2021).

2.2.2 Digitalized Behavior

At the core of digital surveillance are the monitoring and analysis of workers' digitalized behaviors – that is, work-related activities that are performed with the help of or entirely through digital technologies, and which, in turn, are transformed into digital trace data. Digital trace data is typically equipped with granular information about what was done, by whom, and at what point in time. Such trace data can be used to analyze individual actors' behavior as well as to identify larger patterns in datasets that reflect the behavior of collectives of actors. These insights can be used to analyze, evaluate, and manage employees' behaviors (Bernstein 2017; Kalischko and Riedl 2021; Mettler 2023).

Research as well as media reports suggest how various work-related behaviors can be subject to digital surveillance. In office environments, applications can monitor keystrokes (Ball 2021), collect information about web-browsing activities (Saner 2018) or record, store, and analyze various aspects of work-related behavior (Woodcock 2016). In environments requiring physical labor, organizations can use video cameras (Zickuhr 2021) or collect various sorts of biophysical information, such as heart rate or tone of voice (Mettler 2023; Saner 2018). Employees who work outside clearly defined organizational boundaries – such as in food or package delivery – can be monitored by means of sensors that track their movements (Newlands 2021). Emerging digital technologies, such as smart embedded devices, big data analytics, and the IoT provide ever-increasing means for digitalizing behavior by providing granular, high-frequency data in near real time (Seidel and Berente 2020).

However, traces of digitalized behavior represent only certain aspects of the larger reality of a given organization and are only proxies for the actual situation (Flyverbom 2022). Especially in cases where work-related behavior is only partially digitalized, the resulting digital traces may be "imperfect measures" (Mateescu and Nguyen 2019, p. 13). For example, time-related assessments of worker behavior may not consider adverse conditions in the environment that a worker must cope with but cannot change (Newlands 2021). Generally, the more behavior is digitalized, the more aspects of work-related behavior are covered by digital trace data.

2.2.3 Watchers and the Watched

Digital surveillance involves some form of top-down relationship in which one entity (human or machine or any combination thereof) watches another entity (again, human or machine or any combination thereof) – a *watcher* and the *watched* (Zorina et al. 2021). Those who are watched are often employees who may work in any of a variety of work contexts, such as delivery service workers, call center agents, or warehouse workers. We can locate digitally surveilled behavior on a continuum from predominantly manual to fully digitalized. The former implies that only some aspects of work are being performed using digital technologies while the latter means that every relevant aspect of work-related behavior is enabled by digital technologies. While those who are watched are often unaware of what data is collected and for what purposes, contemporary research shows how employees express resistance in relation to digital surveillance by, for example, refraining from using certain digital technologies or intentionally using them to feign desirable behavior (De Vaujany et al. 2021; Newlands 2021). However, it has also been reported that employees tolerate or even desire digital surveillance when they perceive advantages for their position in the organization (Gierlich-Joas et al. 2024; Spicer 2017).

Those who watch have some legitimacy in surveilling others' behavior, which is typically provided by their position in the organizational hierarchy that requires them to manage and supervise the work of others (i.e., those who are watched). Watchers may also be involved in the design, implementation, and control of digital surveillance measures (Anteby and Chan 2018; Park 2021). They may have more information about the form of collected data than those who are watched do (Flyverbom 2022). However, the roles of watchers and the watched may not be entirely clear in a given work setting: Those who are watched can also be watchers, and those who watch others can also be watched. A shift leader in a manufacturing company may surveil

workers' behavior but can also be watched by superordinate managers.

2.2.4 *Digital Processor(s)*

Digital surveillance in organizations is enabled by one or more digital processors that analyze digitalized behavior and provide actionable insights (Leonardi and Treem 2020; Newlands 2021). A digital processor – some combination of hardware and algorithms that transform inputs into outputs – implements watchers' expectations and needs by means of specific encoded algorithmic principles (Park 2021). Digital processors can enable digital surveillance to different extents. They can provide descriptive representations to highlight the features of a digital trace data set such as through specific metrics or visualizations (Flyverbom 2022). Such digital processors have little capacity to act on their own, so the sensemaking and decision making is in the purview of human watchers (or perhaps other machine watchers that use that information). However, as the volume of data increases and surveillance initiatives become more sophisticated, watchers may use digital processors that not only analyze the behavior of those who are watched but also process that information to make management decisions and thus provide the conditions for algorithmic management (Benlian et al. 2022). Such digital processors may be able, for example, to automatically set pay cuts or even fire employees who do not meet expected performance thresholds (Lecher 2019). These applications capitalize on advances in AI, most notably in terms of machine learning and predictive analytics, and have growing degrees of agency to automate complex tasks (Berente et al. 2021).

As new features are invented and implemented, organizations are increasingly capable of performing additional analyses to surveil employees' behavior (Park 2021). These features can also be applied to existing data sources and organizations can thus retrospectively analyze them and make predictions based on historical data. Additionally, organizations can constantly experiment with and introduce new metrics that may provide insights into the behavior of those who are watched.

Figure 1 summarizes the features of digital surveillance in organizations and highlights how digitalized behaviors provide the data streams for digital processors owned by the watchers who, in turn, can use the processors' analyses of the data to influence the behavior of those who are watched.

3 Forms of Digital Surveillance in Organizations

We distinguish different forms of digital surveillance that are established between those who are watched and those who watch the behavior of others. Our model rests on two observations. First, the behavior of those who are watched is digitalized to varying extents, ranging from predominantly manual (with limited involvement of digital technologies) to fully digitalized (i.e., all relevant aspects of work are supported through or enabled by digital technologies). The degree of digitalization determines the volume and detail of digital trace data that provides the basis for watchers to perform digital surveillance. We refer to this as the level of digitalization of behavior.

Second, the digital processor(s) used for analyzing the collected digital traces can support analyses at different levels. These processors may have basic capabilities that enable them to describe and represent performance-related insights (e.g., enabling human watchers to inspect visualizations). More advanced digital processors, such as machine learning-based systems, can provide recommendations or even take actions without human intervention (e.g., automated analysis of patterns, predictive analysis, including decision making). We refer to this as the level of digital processing. Taken together, these two observations lead us to identify four types of digital surveillance (Table 1).

3.1 Digitally Supported Surveillance

Digitally supported surveillance occurs in situations where both the behavior of those who are being watched and the surveillance performed by watchers involve digital technologies to a limited extent. This is the case in organizations that are not "born digital" but introduce digital technologies to improve established processes. In some situations, established organizations may find that certain digital traces are readily available for surveillance, such as the analysis of keystrokes. In other situations, sensors, such as video cameras, can be added to existing work settings, thus representing the surveilled situation (Anteby and Chan 2018). Because workers' behavior is only partially digitalized, the collected digital traces provide a partial and incomplete representation. Additionally, the analyses made by digital processors are not fully automated, such as when watchers manually explore data streams generated by digital sensor acting as a proxy for the actual surveilled process. As indicated earlier, a partial digitalization of work-related behavior can be problematic when the available data is interpreted as objective measures of work-related behavior (Mateescu and Nguyen 2019).

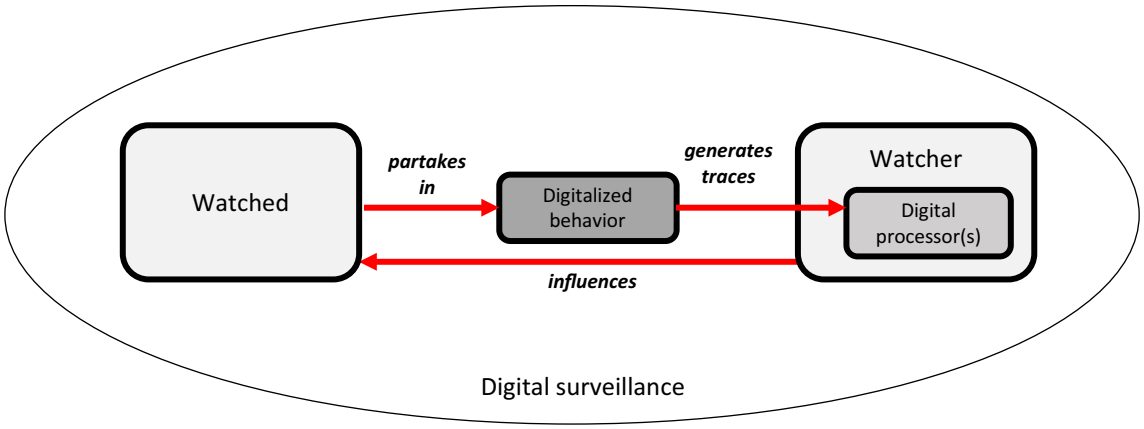

Fig. 1 Features of digital surveillance in organizations

Table 1 Types of digital surveillance in organizations

		Level of digital processing	
		Low	High
Level of digitalization of behavior	Low	**Digitally supported surveillance** *Focus:* Using digital means to improve surveillance by collecting and analyzing digital trace data as proxies for behavior *Example:* Monitoring keystrokes, e-mail, and/or Internet usage	**Analytical digital surveillance** *Focus:* Leveraging advanced analysis tools to process limited sources of digital traces that serve as proxies for work-related behavior *Example:* Dashboards with visualizations and other features to evaluate work-related behavior
	High	**Digitally sourced surveillance** *Focus:* Drawing from digitalized work including sensors to generate comprehensive streams of digital trace data for analysis *Example:* Industrial IoT system that collects information about process activities at a granular level and at high frequency	**Autonomous digital surveillance** *Focus:* Monitoring work-related behavior through sensors, learning from observed data, and pro-actively influencing the process *Example:* AI-based coaching where real-time analytics nudge people to consider their task-related behavior based on the active surveillance of the person's workstream

3.2 Digitally Sourced Surveillance

Digitally sourced surveillance occurs when watchers draw from digital traces that represent a large share of work-relevant behavior, so watchers obtain a good approximation of work performance. At the same time, the digital processors for conducting digital surveillance are not highly advanced. This is the case, for instance, in "born digital" organizations, where most behavior is digitally enabled, but the organization has not invested in advanced digital processors, such as machine-learning-based systems. Examples include IoT-based implementations in manufacturing settings that track key measures of the production process (Serror et al. 2020).

3.3 Analytical Digital Surveillance

Analytical digital surveillance occurs when watchers can draw on advanced means for analyzing surveillance data, but the surveilled behavior is not highly digitalized. Hence, a restricted volume of digital traces serves as proxies for the work activities performed by those who are watched. This is, for instance, the case when manufacturing organizations invest in advanced digital processors but do not have the sensors in place to provide a good approximation of all work-relevant aspects. Such implementations may, for instance, lack granularity and frequency. As with digitally supported surveillance, a danger lies in the available data being interpreted as objective measures of work-related behavior (Mateescu and Nguyen 2019). This issue can be particularly problematic if watchers rely heavily on the analytical means because they are using advanced

methods but, at the same time, have little awareness that the underlying informational basis is incomplete.

3.4 Autonomous Digital Surveillance

Autonomous digital surveillance occurs when fully digitalized processes provide the informational basis for autonomous learning and decision-making. Autonomous digital surveillance requires that behavior is digitalized to a large extent, so data streams cover work-relevant aspects and analytical methods can use these data streams to build analytical models, including predictive models, to support decision-making (Park 2021). Algorithms surveil and autonomously control a variety of online and purely digital domains, such as bots that control open-source software or online communities, and similar technologies are fast becoming possible in physical domains as well. As digital processors can make their own decisions based on analyzing this data, they take on the role of the watcher. Uber famously surveils drivers and controls routes algorithmically (Möhlmann et al. 2021), and digital "nudges" are increasingly replacing overt control (Amar et al. 2022). We can readily conceive of situations in which the informational basis is used for generative activities using recent advances in generative AI.

4 Research Agenda and Ways Forward

Digital surveillance in organizations is an emerging phenomenon at the nexus of technical, organizational, regulatory, and ethical questions (Ajunwa et al. 2017; Flyverbom 2022; Kidwell and Sprague 2009). Studying digital surveillance in organizations requires the consideration of a variety of aspects. Based on the model and the forms of digital surveillance introduced above, we suggest several avenues for future research. They are summarized in Table 2, along with examples of research questions.

4.1 Establishment of Digital Surveillance and Transition between Forms

Research on the design and implementation of digital surveillance in organizations is limited. Certainly, research on the design and implementation of information systems in general is abundant, but how these new forms of digital surveillance are similar to or different from previous waves of information technologies warrants further attention.

Also, it is important to remember that organizations can employ different forms of digital surveillance. Here, we point to two relevant perspectives. First, studying how, why, and when an organization establishes digital surveillance can help unpack the conditions, processes, and outcomes of digital surveillance. One can study the core motives and expectations of managers who decide to analyze digitalized behavior and whether digital surveillance in organizations is necessarily planned or can emerge over time as managers recognize means for digital surveillance.

Second, one could study how, why, and when an organization shifts between forms of digital surveillance. Such shifts can relate to the types of behaviors that can be monitored, the collected data, and the analytical methods in use. For example, an organization may initially employ digitally supported surveillance, but may capitalize over time on more digital trace data streams and use more sophisticated digital processors, establishing more advanced forms of digital surveillance, such as analytical digital surveillance or even autonomous digital surveillance.

Furthermore, future research could study digital surveillance across organizations and industries and in relation to various populations. For example, industries like food or package delivery services may be particularly prone to digital surveillance initiatives (Zickuhr 2021). Future studies should also consider that digital surveillance in organizations may also have empowering implications (Gierlich-Joas et al. 2024).

4.2 Relationships among Watchers and the Watched

At least two roles are necessary for digital surveillance to occur: those whose behavior is being watched and those who watch the behavior of others. Digital surveillance initiatives in organizations may prompt the development of new roles, routines, and strategies over time (Zorina et al. 2021). For example, watchers may introduce new metrics as proxies for inferring employees' productivity, such as idle times during which mouse cursors are not moved (Zickuhr 2021). Such developments may lead to unintended consequences, such as when service workers in call centers start to behave in ways that satisfy the digital processor but confuse the customer by, for example, apologizing unnecessarily often or maintaining a tone of voice that is unaligned with the call's content (Dzieza 2020). Digital surveillance in organizations is often associated with stress (Newlands 2021), especially when the behavior of those being watched is punished while, at the same time, the actual reason for that punishment is not clear (Zickuhr 2021).

Increasing interest is shifted to the role of those who are being watched (e.g., Ball 2021; De Vaujany et al. 2021; Manley and Williams 2019; Newlands 2021), but fully understanding digital surveillance in organizations requires to also understanding the watchers' motives and practices, and how they change over time. For example, the ability to perform surveillance is inextricably linked to power, so

Table 2 Research avenues and examples of questions to study digital surveillance in organizations

Research avenues addressing digital surveillance in organizations	Examples of questions for future research
Establishment of digital surveillance and transition between forms	Why and when do organizations move from one form of digital surveillance to another?
	How do digital surveillance initiatives in organizations evolve over time, e.g., when do watchers recognize new means for digital surveillance?
	To what extent is digital surveillance related to the forms of organizations and industries?
Relationships between watchers and the watched	How does digital surveillance lead to power shifts in organizations?
	How does the dual role of watcher and watched influence workers' actions and motives?
	What are ethical implications for information systems researchers in design-oriented research projects?
Responses and consequences	How does digital surveillance in organizations disempower and empower?
	What are the effects of digital surveillance, including compliance, resistance, and gaming?
	What is the impact of digital surveillance on organizational outcomes, including productivity, financial outcomes, and competitive outcomes, as well as on political dynamics and cultural implications?
Roles of digital processors	How do advancements in machine learning change and expand opportunities for digital surveillance in organizations?
	How do watchers and the watched react to decisions of AI-based digital technologies when they cannot fully understand how these decisions were made?
	How do built-in features in third-party digital technologies provide standardized digital surveillance approaches across organizations and industries?
The means to digitalize behavior	What types of digital trace data are more or less useful for digital surveillance in organizations?
	Through which channels do watchers collect data to exert surveillance?
	How does digital surveillance interfere with privacy concerns, and how do those who are watched preserve privacy?

future research could study whether or to what extent power relations change after the implementation of digital surveillance initiatives. One could also study the role of corruption, for instance, by examining whether and how watchers circumvent or even ignore regulations as they surveil employees' behavior (Zuboff 2019). Furthermore, attending to the role of those who design, implement, or curate digital surveillance initiatives, such as data science teams (Pachidi et al. 2021), is important because such teams may take on key roles in digital surveillance initiatives as they gain access to a sensitive data, both produced by employees and managers.

Another issue that warrants attention is that in many work settings, employees are both watchers *and* watched. As more and more work-related behavior is digitalized across various hierarchical levels, the work of one employee may be watched by others while his/her own work description may involve surveilling others. An example are middle managers who are responsible for tracking and monitoring the work performance of their subordinates, but whose own performance, in turn, can be watched by their superiors. One angle for future research is to study how one's own surveillance activities may influence attempts to hide from or influence traces that are analyzed by others.

A more subtle implication pertains to the role we play as researchers, for instance, when we conduct design science research (Mettler 2023). When such projects seek to make the behavior of certain workgroups visible, or to even evaluate or manage their behavior, we must be aware of any ethical implications that may arise from that research, such as when we present insights to managers who may be interested in watching their employee's behaviors or when a designed system is used in practice (Mettler 2023).

4.3 Responses and Consequences

Organizations implement digital surveillance in the service of productivity and efficiency as well as to accomplish regulatory compliance. Future research should explore to what extent these goals are achieved, how they are achieved, and at what cost. For example, surveillance can reduce the level of trust between managers and employees (Taekke 2011), but what is the cost of this reduced trust? Research should seek to understand the consequences and dynamics of responding to and appropriating digital surveillance over time. Responses to control technologies

vary (e.g., Berente et al. 2019; Yates 1993), but to what extent digital surveillance allows for the same or similar reactions and in what way they differ, is unclear. For example, contemporary research stresses how those who are being watched engage in resistance or manipulate data to blur their actual behavior (e.g., Bernstein 2017; Newlands 2021). At the same time, it has been emphasized "how enthusiastic employees are about being watched through ever more invasive technology" (Spicer 2017). Media reports suggest, for instance, that younger generations are often willing to limit their privacy (Saner 2018; Spicer 2017).

4.4 Roles of Digital Processors

We highlighted the role of digital processors in analyzing, evaluating, and acting on digital traces that are collected during work-related behavior. These technologies can take various forms and are capable of taking over various tasks ranging from the simple representation of data-based insights to automated and independent decisions that directly affect the behavior of those who are watched (Mateescu and Nguyen 2019; Park 2021). Digital technologies are expected to have increasing degrees of agency (Park 2021), turning them into "machineries of knowing" (e.g., Flyverbom 2022) that can act autonomously.

This observation has several implications for future research. First, future research could study how specifically AI is used for digital surveillance in organizations. To this end, one could study how those who watch as well as those who are watched react to decisions about the use of AI, as AI is often inscrutable (Berente et al. 2021). Future research could also attend to the fact that digital processors are often provided by third-party providers that give watchers access to a variety of work-related data (Kalischko and Riedl 2021) and develop and offer tools to evaluate the workers' performance. Consider, for example, how productivity evaluations of collaboration platforms can be associated with surveillance features (Hern 2020). If such metrics become standardized across organizations and even industries, we can expect that organizations converge in their digital surveillance practices, and future research could study the outcomes of that convergence.

4.5 The Means to Digitalize Behavior

As more and more work-related aspects are being supported by or enabled by digital technologies, we can expect that organizations will develop more extensive means to employ digital surveillance in the future (Zickuhr 2021). Future research could investigate how the different types of such traces lead to different insights about the behavior of those being watched. One could also examine what kinds of patterns and motives can be inferred from digital trace data streams to inform managerial insights and decision-making. To this end, Flyverbom (2022) urges us to shift our attention from content (i.e., what is surveilled) to *conduit*, that is, the channels employees use when they work and from which data can be collected for surveillance purposes.

For example, one could study how the increasing digitalization of behavior affects privacy and can lead to the development of technologies to protect privacy and comply with privacy-related regulations. Privacy refers here to the degree to which those who are watched have the ability to control information about themselves (Awad and Krishnan 2006). As work is increasingly performed with digital technologies, and as technological advancements of digital processors enable novel means to monitor, analyze, and evaluate the behavior of those who are watched, organizations will likely further restrict the privacy of those who are watched (Ball 2021), which will widen the information asymmetry associated with digital surveillance in organizations. While those who watch gain possession of larger amounts of digital traces from a growing number of sources and increasingly powerful computational means to analyze them, those who are being watched will become increasingly unaware of what is known about them and how their behavior informs managerial decisions (Flyverbom 2022; Park 2021). Consider digital processors that enable "reputation surveillance" (Zickuhr 2021), that is, monitoring employees' behavior well beyond the work context, such as by evaluating their posting behavior on their private social media profiles (Weber 2014). There are also technical solutions to problems like privacy, such as differential privacy, which is often touted as a means to satisfy requirements for data while at the same time preserving privacy (Kearns and Roth 2019).

5 Conclusion

As work-related behavior becomes more and more digitalized and transformed into digital traces, organizations increase the digital surveillance of their employees. We conceptualize key features of digital surveillance in organizations and suggest that it can take different forms based on the availability of digital trace data and digital processes. We point to several future research opportunities for information systems researchers.

Funding Open Access funding enabled and organized by Projekt DEAL.

References

Ajunwa I, Crawford K, Schultz J (2017) Limitless worker surveillance. Cal Law Rev 105:735–776

Amar J, Majumder S, Surak Z, von Bismarck N (2022) How AI-driven nudges can transform an operation's performance. https://www.mckinsey.com/capabilities/operations/our-insights/how-ai-driven-nudges-can-transform-an-operations-performance#/. Accessed 28 Mar 2024

Anteby M, Chan CK (2018) A self-fulfilling cycle of coercive surveillance: workers' invisibility practices and managerial justification. Organ Sci 29(2):247–263

Awad NF, Krishnan MS (2006) The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization. MIS Q 30(1):13–28

Ball K (2021) Electronic monitoring and surveillance in the workplace. Literature review and policy recommendations. https://publications.jrc.ec.europa.eu/repository/handle/JRC125716. Accessed 28 Mar 2024

Benlian A, Wiener M, Cram WA et al (2022) Algorithmic management: bright and dark sides, practical implications, and research opportunities. Bus Inf Syst Eng 64(6):825–839

Berente N, Lyytinen K, Yoo Y, Maurer C (2019) Institutional logics and pluralistic responses to enterprise system implementation: a qualitative meta-analysis. MIS Q 43(3):873–902

Berente N, Gu B, Recker J, Santhanam R (2021) Managing artificial intelligence. MIS Q 45(3):1433–1450

Bernstein ES (2017) Making transparency transparent: the evolution of observation in management theory. Acad Manag Ann 11(1):217–266

Boyne R (2000) Post-panopticism. Econ Soc 29(2):285–307

Ciborra C (2000) From control to drift: the dynamics of corporate information infastructures. Oxford University Press

Clarke R (1988) Information technology and dataveillance. Commun ACM 31(5):498–512

Clarke R (2019) Risks inherent in the digital surveillance economy: a research agenda. J Inf Technol 34(1):59–80

Clegg SR (1981) Organization and Control. Adm Sci Q 26(4):545–562

De Vaujany F-X, Leclercq-Vandelannoitte A, Munro I, Nama Y, Holt R (2021) Control and surveillance in work practice: cultivating paradox in 'new'modes of organizing. Organ Stud 42(5):675–695

Dzieza J (2020) How hard will the robots make us work? The Verge, 27 Feb 2020. https://www.theverge.com/2020/2/27/21155254/automation-robots-unemployment-jobs-vs-human-google-amazon. Accessed 28 Mar 2024

Elmes MB, Strong DM, Volkoff O (2005) Panoptic empowerment and reflective conformity in enterprise systems-enabled organizations. Inf Organ 15(1):1–37

Flyverbom M (2022) Overlit: digital architectures of visibility. Organ Theor. https://doi.org/10.1177/26317877221090314

Foucault M (1977) Discipline and punish: the birth of the prison. In: Alan Sheridan (ed) Vintage Books, New York

Gartner (2019) The future of employee monitoring. https://www.gartner.com/smarterwithgartner/the-future-of-employee-monitoring. Accessed 28 Mar 2024

Gierlich-Joas M, Baiyere A, Hess T (2024) Inverse transparency and the quest for empowerment through the design of digital workplace technologies. J Assoc Inf Syst, forthcoming

Grey C (1994) Career as a project of the self and labour process discipline. Soc 28(2):479–497

Hern A (2020) Microsoft productivity score feature criticised as workplace surveillance. The Guardian. https://www.theguardian.com/technology/2020/nov/26/microsoft-productivity-score-feature-criticised-workplace-surveillance. Accessed 28 Mar 2024

Kalischko T, Riedl R (2021) Electronic performance monitoring in the digital workplace: conceptualization, review of effects and moderators, and future research opportunities. Front Psychol 12:633031

Kearns M, Roth A (2019) The ethical algorithm: the science of socially aware algorithm design. Oxford University Press

Kidwell RE, Sprague R (2009) Electronic surveillance in the global workplace: laws, ethics, research and practice. New Technol Work Employ 24(2):194–208

Lecher C (2019) How Amazon automatically tracks and fires warehouse workers for 'productivity'. The Verge, 25 Apr 2019. https://www.theverge.com/2019/4/25/18516004/amazon-warehouse-fulfillment-centers-productivity-firing-terminations. Accessed 28 Mar 2024

Leonardi P, Treem J (2020) Behavioral visibility: a new paradigm for organization studies in the age of digitization, digitalization, and datafication. Organ Stud 41(12):1601–1625

Manley A, Williams S (2019) 'We're not run on numbers, we're people, we're emotional people': exploring the experiences and lived consequences of emerging technologies, organizational surveillance and control among elite professionals. Organization 29(4):692–713

Mateescu A, Nguyen A (2019) Algorithmic management in the workplace. https://datasociety.net/library/explainer-algorithmic-management-in-the-workplace/. Accessed 28 Mar 2024

Mettler T (2023) The connected workplace: characteristics and social consequences of work surveillance in the age of datification, sensorization, and artificial intelligence. J Inf Technol. https://doi.org/10.1177/02683962231202535

Möhlmann M, Zalmanson L, Henfridsson O, Gregory RW (2021) Algorithmic management of work on online labor platforms: when matching meets control. MIS Q 45(4):1999–2022

Newlands G (2021) Algorithmic surveillance in the gig economy: the organization of work through Lefebvrian conceived space. Organ Stud 42(5):719–737

Pachidi S, Berends H, Faraj S, Huysman M (2021) Make way for the algorithms: symbolic actions and change in a regime of knowing. Organ Sci 32(1):18–41

Park YJ (2021) The future of digital surveillance: why digital monitoring will never lose its appeal in a world of algorithm-driven AI. University of Michigan Press, Ann Arbor

Rosenblat A, Kneese T, Boyd D (2014) Workplace surveillance. Open Society Foundations' Future of Work Commissioned Research Papers. https://www.datasociety.net/pubs/fow/WorkplaceSurveillance.pdf. Accessed 28 Mar 2024.

Saner E (2018) Employers are monitoring computers, toilet breaks – even emotions. Is your boss watching you? The Guardian.

https://www.theguardian.com/world/2018/may/14/is-your-boss-secretly-or-not-so-secretly-watching-you. Accessed 28 Mar 2024

Seidel S, Berente N (2020) Automate, informate, and generate: affordance primitives of smart devices and the internet of things. In: Nambisan S, Lyytinen K, Yoo Y (Eds.), Handbook of digital innovation, Elgar, pp 198–210, Edward Elgar Publishing, Cheltenham, UK

Serror M, Hack S, Henze M, Schuba M, Wehrle K (2020) Challenges and opportunities in securing the industrial internet of things. IEEE Trans Ind Inform 17(5):2985–2996

Spicer A (2017) Surveillance used to be a bad thing. Now, we happily let our employers spy on us. The Guardian, 4 Aug 2017. https://www.theguardian.com/commentisfree/2017/aug/04/surveillance-employers-spy-implanted-chipped. Accessed 28 Mar 2024

Taekke J (2011) Digital panopticism and organizational power. Surveill Soc 8(4):441–454

Weber J (2014) Should companies monitor their employees' social media? The Wall Street Journal, 22 Oct 2014. https://www.wsj.com/articles/should-companies-monitor-their-employees-social-media-1399648685. Accessed 28 Mar 2024

Woodcock J (2016) Working the phones: control and resistance in call centres. Pluto Press, London

Yates J (1993) Control through communication: the rise of system in American management, vol 6. JHU Press

Zickuhr K (2021) Workplace surveillane is becoming the new normal for U.S. workers. https://equitablegrowth.org/. Accessed 28 Mar 2024

Zorina A, Bélanger F, Kumar N, Clegg SR (2021) Watchers, watched, and watching in the digital age: reconceptualization of information technology monitoring as complex action nets. Organ Sci 32(6):1571–1596

Zuboff S (1988) In the age of the smart machine: the future of work and power, vol 186. Basic Books, New York

Zuboff S (2019) The age of surveillance capitalism: the fight for a human future at the new frontier of power. Profile Books, New York