

# ‘This might sound like I’m wearing a tinfoil hat...’ – Knowledge workers’ perceptions of privacy and surveillance in group-based communicative AI

Convergence: The International  
Journal of Research into  
New Media Technologies  
2025, Vol. 0(0) 1–20  
© The Author(s) 2025



Article reuse guidelines:  
[sagepub.com/journals-permissions](https://sagepub.com/journals-permissions)  
DOI: 10.1177/13548565251410408  
[journals.sagepub.com/home/con](https://journals.sagepub.com/home/con)



Liisa A. Mäkinen<sup>1</sup> , Minna Koivula<sup>1</sup>  and Mia Leppälä<sup>1</sup> 

## Abstract

This study examines knowledge workers’ perspectives on privacy implications and surveillant functionalities of group-based communicative AI in the context of work. The objective is to connect the ongoing examination of communicative AI in the workplace to research on privacy and employee surveillance, and to use the framework of privacy as contextual integrity as a theoretical lens through which some of the user perspectives on communicative AI tools are analyzed. Building on 33 qualitative interviews with Finnish knowledge workers, who were presented with scenarios of communicative AI functioning as a ‘team member’ in a work-related chat group, we find that knowledge workers recognize several privacy-related risks in using group-based communicative AI at work, and commonly use surveillant reasoning and logics to make sense of the suggested technology and its privacy implications. We present three distinct approaches knowledge workers had toward privacy in this setting: the detached, the compartmentalized, and the affective. Our findings suggest a wider need to consider communicative AI’s agency and role as an actor contributing to increasing privacy concerns. We highlight how, due to its human-like nature, data-reliant functionalities, and potential capabilities when operating in a group setting, the technology introduces negative affective responses and novel concerns related to privacy and employee surveillance. Specifically, privacy concerns relating to communicative AI expand beyond mere data protection issues to include concerns of how the technology is used by management, how the technology itself interacts within the organization, and how it will develop in the future.

## Keywords

communicative AI, teamwork, group discussions, workplace, privacy, surveillance, datafication, qualitative research

---

<sup>1</sup>Centre for Consumer Society Research, University of Helsinki, Helsinki, Finland

## Corresponding author:

Liisa A. Mäkinen, Centre for Consumer Society Research, University of Helsinki, P.O. Box 16 (Snellmaninkatu 10), FI-00014, Helsinki, Finland.

Email: [liisa.x.makinen@helsinki.fi](mailto:liisa.x.makinen@helsinki.fi)

## Introduction

Communicative AI has swooshed into workplaces as a technology that can aid in multiple different tasks ranging from translations and language assistance to organizing and systematizing information to producing content, aiding in creative processes, and operating as a conversation partner (Gilmore et al., 2025; Gkinko and Elbanna, 2022; Heuser and Vulpius, 2024; Mahnke, 2024; Mahnke and Bagger, 2024; Ramaul et al., 2024). As a technology, communicative AI builds on Large Language Models (LLMs) and is ‘designed to carry out specific tasks within the communication process that were formerly associated with humans’ (Guzman and Lewis, 2020: 22). Depending on the context, it has been termed generative AI, GenAI or GAI, conversational agent, social robot, or automated-writing software (Guzman and Lewis, 2020). By nature, communicative AI tools are based on large amounts of data and their operations build on collecting, combining, storing, and sharing data. Thus, considerations regarding privacy are pertinent when examining not only how the technology operates and is used, but also how users relate to and make sense of it. User perspectives on privacy implications of communicative AI have not yet been in the focus of empirical investigation. This study examines knowledge workers’ perspectives on privacy implications and surveillant functionalities of communicative AI in the context of work, with a specific focus on the ramifications of communicative AI’s future developments into teamwork.

Employee surveillance in itself is nothing new, as workers have always been subjected to many forms of monitoring and control (Ball, 2010). However, the recent shift to remote work due to the pandemic, alongside increasing datafication of work and advancements made in sensorization and artificial intelligence (AI) have changed and increased employee surveillance practices (Cousineau et al., 2023; Mettler, 2024). Datafication, in particular, has created new kinds of opportunities for monitoring employees: increasing amounts and varieties of digital data available on employees allows for new ways for employers to monitor them. Surveillant logics are embedded in datafication practices, as transforming social practices into quantified data also allows for ‘real-time tracking and predictive analysis’ (Van Dijck, 2014: 198; Mayer-Schönberger and Cukier, 2013). The proliferation of datafication has also paved the way for communicative AI technology (see e.g. Mahnke and Bagger, 2024). While communicative AI tools in general are not designed as surveillance devices (in the sense that their reason for existence would be to gather information on the user in order to control or manage them or to modify their behaviour), their operations build on collecting, storing, organizing, and using data in a manner that is often invisible to the user and can affect their behaviour. Furthermore, the human-like nature of communicative AI can ‘obscure the complex datafication processes, power asymmetries, and potential biases embedded in GenAI platforms’ (Mahnke and Bagger, 2024: 1975). The data-reliant functionalities of communicative AI technology, as we will demonstrate in this article, render many users to perceive this technology as a surveillance tool.

Thus far, most studies examining the everyday uses and users’ perspectives toward communicative AI have focused on a one-on-one setting (see e.g. Gkinko and Elbanna, 2022; Heuser and Vulpius, 2024; Mahnke, 2024; Mahnke and Bagger, 2024), where privacy risks are often conceptualized as data protection issues or relating to data ownership (Das et al., 2025; Gilmore et al., 2025; Gupta et al., 2023; Lucia et al., 2025). For this study, we created scenarios of communicative AI operating in a group chat and examined employees’ privacy concerns regarding their personal data, communication practices, and social relationships. Based on interviews with Finnish knowledge workers from different fields, we analyze how employees make sense of communicative AI technology, what kinds of data they perceive as ‘risky’ or sensitive, and how they approach privacy risks associated with group-based communicative AI in the workplace. The question this research seeks to answer is: How do knowledge workers approach and understand privacy in relation

to group-based communicative AI at work. This study has two objectives: First, to connect the ongoing examination of communicative AI in the workplace to research on privacy and employee surveillance, with a focus on the framework of privacy as contextual integrity (Nissenbaum, 2010); and second, to present an empirical analysis of knowledge workers' approaches to privacy-related consequences and surveillance implications of communicative AI in the workplace.

## Workplace surveillance and datafication of work

Employees are habitually subjected to many forms of surveillance and have even come to expect it as part of good management practice. In the context of work, surveillance has been defined as the employers' ability to monitor, track, and record employees in various ways either in real time or as part of larger organizational processes (Ball, 2010). Employee surveillance can include monitoring work performance and tasks (e.g. measuring outputs or activities), behaviour and thoughts (e.g. tracking location or communication practices), and/or personal characteristics, activities, and reputation (e.g. conducting drug and alcohol tests, monitoring biometrics, or covertly assessing worker conduct) (Ball, 2010, 2021, 2022; Cousineau et al., 2023; Ravid et al., 2020). Employee surveillance can be conducted purposefully or as part of other organizational processes, and it can be continuous, intermittent, or random, discreet or intrusive, and take place with or without consent (Ravid et al., 2020). Furthermore, it can be seen as an organizing principle that functions based on hierarchies and is at times 'veiled in organizing processes' (Ball, 2022: 456). Employee surveillance, as argued by Ball (2010: 97), is 'embedded within organizations, signifies different meanings, and can be appropriated by both workers and managers in the negotiated reality of working life'.

Amongst recent developments in the digital ecosystem, datafication is the one that has perhaps affected work surveillance the most. Datafication, in general, is understood as the practice of collecting and storing quantified information which is then arranged and analysed with the purpose of creating new knowledge and economic value (Mayer-Schönberger and Cukier, 2013). The practices of digitalization, namely, datafication and platformization, create new opportunities for workplace surveillance: increasing amounts and varieties of employee digital data allow for novel ways for employers to monitor them. Furthermore, datafication has further embedded surveillance into organizational practices (Ball, 2022). This process operates as a circle: digitalization enables building employee surveillance systems based on algorithms, which accelerates datafication of work (Cousineau et al., 2023). This, in turn, brings forth new surveillance possibilities and new avenues for datafication, which again increases different surveillance possibilities. Workplace datafication is thus, at least in part, enacted through surveillance technologies (Cousineau et al., 2023).

Datafication allows for 'a heightened visibility of employees and their activities through data' (Ball, 2021: 10) as datafication practices span beyond individual performance details to include worker characteristics and behaviours. This type of 'connected workplace surveillance' (Mettler, 2024) is not limited to work-related data, physical workplace, or even the employee themselves. Contemporary digital surveillance of work increasingly means monitoring various data practices and communications. Thus, employee surveillance is not necessarily operated only through dedicated surveillance equipment, but all kinds of digital technologies used at work have the potential to be data sources. Furthermore, contemporary digital employee surveillance practices expand from physical workplaces into online social spaces making the distinction between work and personal life hard to establish: As employee surveillance reaches into homes and other private places, it does not target merely the employee but simultaneously increases the visibility of family members and close contacts (Ball, 2021; Cousineau et al., 2023; Mettler, 2024). These developments lead to the spatial,

temporal, and relational blurring of boundaries between work and personal life (Cousineau et al., 2023).

Businesses have an incentive to monitor their employees, and the value of information as an important organizational resource has been recognized long before the possibilities allowed by new technologies emerged (Stanton and Stam, 2003). Indeed, surveillance serves corporate interests in many ways: it can aid in recruiting practices, help maintain productivity and monitor resource use, ensure efficiency, protect trade secrets, shield companies from legal liabilities, and safeguard customer satisfaction (Ball, 2010; Degli Esposti, 2014). Thus, as surveillance is instrumental for organizations in achieving their relevant objectives (Degli Esposti, 2014), organizations are increasingly tempted to collect large and diverse datasets on individual employees from various sources (Ravid et al., 2020), including new digital communication tools.

The full consequences of digital surveillance of work are yet to be determined (Mettler, 2024). Even before the emergence of present day intrusive digital monitoring practices it was noted that workplace surveillance practices ‘can have transformative effects on the occupational experiences of those who are subject to them’ (Ball, 2002: 125). Employee surveillance can affect employee well-being, creativity, productivity, and motivation and even the organization’s work culture: Excessive monitoring can guide which tasks are focused on, reduce employee trust, produce undesired behaviours, and have detrimental effects on employees’ feelings of privacy (Ball, 2010).

### **Privacy boundaries in contemporary datafied work life**

Perhaps the most often stated negative effect of employee surveillance is that it conflicts with employees’ right to privacy (Ball, 2010; Cousineau et al., 2023; Mettler, 2024). Privacy concerns can be seen as especially relevant in the context of work as organizations typically collect substantial amounts of data about their employees’ activities (Stanton, 2003). However, employees’ right to privacy can also be seen as limited because they are operating within their employer’s organizational space and using equipment controlled by their employer (Kidwell and Sprague, 2009; Ravid et al., 2020). This contradiction relates to how privacy in general, and in the context of work, is understood and defined.

In privacy research, privacy has been approached as ‘a claim, a right, an interest, a value, a preference, or merely a state of existence’, and depending on the context, it has been seen as a descriptive, normative, or a legal concept (Nissenbaum, 2010: 2). Some of the classic definitions of privacy see the practices where individuals or groups control information or constrain access to it as the basis for privacy protection (Altman, 1976; Westin, 1967). In legal discourse, particularly pertaining to the digital ecosystem, privacy is commonly conceptualized as informational privacy, meaning data protection. In this framing, privacy is seen to be achieved through managing the processing of personal data with regulation, building protective safeguards within information systems, and providing individuals control over their own data (Bennett, 2008). The challenge in framing privacy as data protection is that it reduces privacy to an issue that can be addressed and solved, for example, through fair information principles. Furthermore, this view does not take into account the subjective nature of experiencing privacy violations (Bennett, 2008; Haggerty and Ericson, 2005) or different contextual settings where privacy is needed.

The notion of different contexts for privacy has been developed particularly by privacy scholar Helen Nissenbaum (2010) in her framework of privacy as contextual integrity, which builds on analyzing social contexts and context-relative informational norms: According to Nissenbaum (2004, 2010), different social contexts are governed by different social norms that prescribe the flow of information within and out of a given context. Nissenbaum (2004) argues that in any context two

types of informational norms apply: norms of appropriateness (what information is appropriate to reveal in any specific context) and norms of flow or distribution (what is appropriate to share from one party to another). Furthermore, she states that ‘context-relative informational norms are characterized by four key parameters: contexts, actors, attributes, and transmission principles’ (Nissenbaum, 2010: 140). Contexts are the social settings where information is shared; actors refer to the subject of information, its sender, or its recipient; attributes refer to the nature and type of the information that is shared; and transmission principles express the terms and conditions under which data are shared (e.g. ‘in confidence’ or ‘as required by law’) (Nissenbaum, 2010, 2015). These parameters help determine whether a particular flow of information in a specific context is appropriate. If informational norms are contravened, individuals experience a privacy violation, or in the vocabulary of the theory, a ‘violation of contextual integrity’ (Nissenbaum, 2010:127). Consequently, protecting privacy entails ensuring that appropriate information flows in an appropriate manner within and between contexts.

Nissenbaum’s theory addresses the often-raised paradox of privacy where people tend to argue that privacy is important to them, yet contradict this claim in their everyday actions (Barnes, 2006). Nissenbaum (2010) argues that if we understand the right to privacy as a right to context-appropriate flows of information, then ‘there is no paradox in caring deeply about privacy and, at the same time, eagerly sharing information’ (Nissenbaum, 2010: 187). Contextual integrity theory is also useful when examining privacy in the workplace and considering why employee surveillance provokes criticism in some instances, but goes unnoticed in others. Controversies surrounding employee surveillance practices have been found to arise especially in situations where monitoring cannot be seen as reasonable or absolutely necessary, when it is too detailed (e.g. monitoring exact time use), or when it ‘negatively affects existing levels of control, autonomy and trust’ (Ball, 2010: 89). Building on these considerations, in the context of work, privacy should be understood in the widest possible sense, ranging from strict data protection and controlling access to information to ensuring privacy in social relationships (including privacy of those close to the employee who might be inadvertently surveilled) and to protecting individual personal space and autonomy (Ball, 2010; Mettler, 2024).

## Communicative AI in the workplace

Forms of artificial intelligence have been a part of work for the better part of two decades, for example, in the form of algorithmic search and recommendations (Söllner et al., 2025). Earlier forms of AI often referred to ranking or classifying content, or the automation of human work (Jarrahi, 2018), whereas current generative AI models are capable of operating as predictive co-creators: The narrative, currently, has turned more toward emphasizing enhancing human capabilities rather than completely substituting human labour (Raisch and Krakowski, 2021; Ramaul et al., 2024). In this study, we understand ‘generative AI’ to refer to machine-learning models capable of producing human-like outputs in the form of text, visual, or audio responses to messages (Brynjolfsson et al., 2025; Feuerriegel et al., 2024). These technologies draw from large datasets, learn patterns and relationships, and operate using probabilities (Feuerriegel et al., 2024). Their capability to produce human-like responses has made them intriguing conversational partners to an increasing number of knowledge workers.

To highlight the communicative nature of generative AI, we use the term *communicative AI* (Guzman and Lewis, 2020). The term usefully emphasizes the technology’s communicative agency (e.g. Sundar and Lee, 2022) as it interacts with knowledge workers in organizational settings. Put differently, communicative AI currently takes part in organizational processes previously ascribed to humans, such as meaning-making, in a way that they become co-creation between the human and the

machine (Guzman and Lewis, 2020; Tang, 2024). Being able to communicate in a similar manner to human employees with some degree of contextual awareness, these technologies have become more approachable than their predecessors (Mahnke, 2024). However, in an organizational context, their implementation also comes with trade-offs relating to, for example, data ownership and privacy: A communicative AI, to function efficiently in an organization, necessitates ongoing access to organizational data, some of which may be private or sensitive in nature (Das et al., 2025; Feuerriegel et al., 2024).

A growing body of literature addresses the use of communicative AI in the workplace, examining how employees have adopted it for professional purposes (e.g. Gilmore et al., 2025; Gkinko and Elbanna, 2022; Mahnke, 2024; Mahnke and Bagger, 2024; Ramaul et al., 2024). On the individual level, these studies show that communicative AI is most often used to assist in language and translations, to organize and systematize information, to produce content, to aid in creative processes, and to operate as a conversation partner (Mahnke, 2024; Mahnke and Bagger, 2024). However, communicative AI adoption has also been shown to be a complex process as is the case with any organizational transformation: Einola et al. (2024), for example, found that the implementation of a bot into a media consultancy company amplified negative collective affects in the organization, ‘which can lead to heightened mutual distrust and blame games’ (Einola et al., 2024: 1641). This was partly fuelled by managers’ and employees’ differing expectations for the technology, managers holding optimistic and employees a pessimist view of its capabilities. A similar sentiment is echoed elsewhere too: Luger and Sellen (2016) have shown that user expectations and actual system capabilities of conversational agents do not usually match, and that the unrealistic expectations tend to frame the disappointing user experience. Relatedly, they found that many users were reluctant to use the technology for complex or sensitive activities.

While public discourse around communicative AI often highlights fear-induced dystopian imaginaries (Lucia et al., 2025), scholars have not yet comprehensively addressed such concerns on the individual level. Specifically, perceived risks relating to surveillance and privacy in communicative AI use have not been studied in detail. In the context of a Southeast Asian NGO, Mahnke (2024) reported that employees expressed concern over loss of authorship, overreliance, and lack of data transparency. In a similar vein, Gupta et al. (2023) note the possibilities of deviant use of the technology in organizations: As tools like ChatGPT are ‘fluent’ in professional discourse, they may be used to manipulate employees through social engineering or reverse psychology. More broadly, AI technologies have been argued to challenge professional identities, considerations of status and forms of collaboration in organizations (Sergeeva et al., 2020) which, given the increasing popularity of these tools in organizational settings (Mahnke and Bagger, 2024), implies a need for continued sensemaking around communicative AI.

## **Methodology**

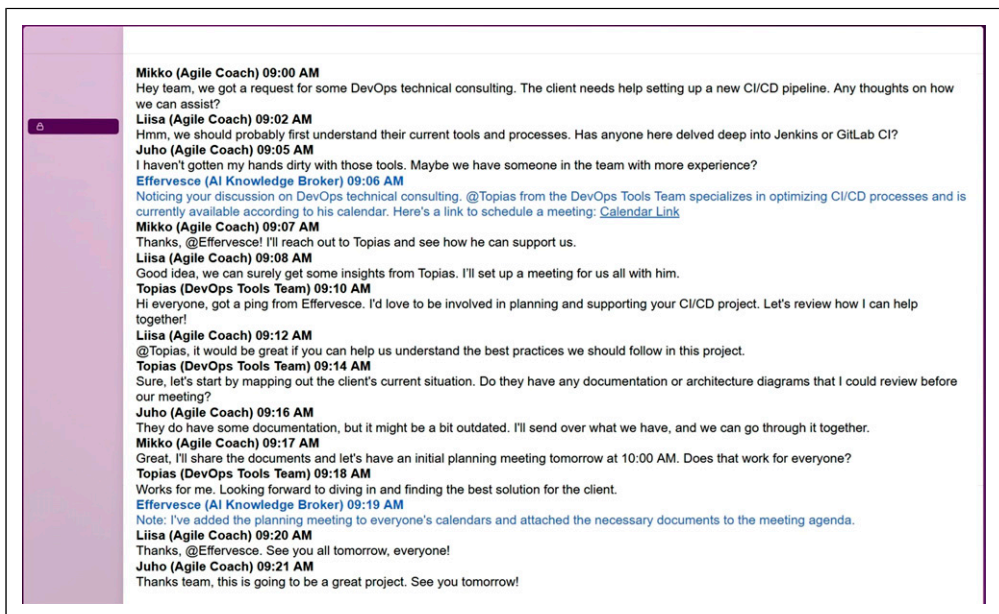
### *Data generation*

To examine perceptions of surveillance and privacy relating to communicative AI at work, we conducted 33 qualitative interviews with Finnish knowledge workers. The interviews were carried out between May and December 2024 and included experts from various fields including media (13 participants), education (7), technology and IT consulting (4), research and development (3), marketing (2), and various industries (4). The knowledge workers self-identified as active users of communicative AI in their work, however, their use was usually characterized by experiences of one-on-one conversations with communicative AI. Seventeen of the interviewees were male and

sixteen were female. We carried out the data collection through Zoom and Teams giving our informants the option to choose which platform to use (see Heiselberg and Stępińska, 2022). The average duration of an interview was 56 minutes. All interviews were recorded and later transcribed to text with the help of AI transcribing software. A research assistant went through the final transcriptions for accuracy. Informants provided written consent to participate in the study and to publish its results. All informants are referred to by pseudonyms in the Findings section.

The interview guide was built around three sections: experiences of communicative AI use, emotions and skills relating to communicative AI as well as future scenarios of communicative AI at work. Being semi-structured, the guide facilitated discussion specifically on the points interviewees felt were important but also allowed for follow-up questions and deviations from the original questions (Tracy, 2020). In this study, our focus is mainly on the final section of the interviews which depicted a selection of scenarios (see e.g. Kieslich et al., 2024), that is, imagined group communication situations, where a communicative AI functioned as a ‘team member’ and aided a team of professionals in their tasks. The scenarios were planned to prompt ideas and reflections on what communicative AI could be in the workplace as well as to specifically capture informant’s thoughts on the technology’s surveillance and privacy implications. We considered this type of prompt-led approach (e.g. Jiménez and Orozco, 2021) suitable for generating insights into the role of communicative AI in a group setting given that none of our participants had used such a group-based tool previously and no such tools were publicly available at the time. Each informant was shown two scenarios. A scenario used as an interview prompt can be seen in Picture 1.

As our informants came from varying organizational contexts, the scenarios were somewhat tailored to suit their work realities: In each scenario, the communicative AI performed the same tasks (such as connecting people in the organization to each other, making notes, scheduling meetings, or brainstorming ideas) while the context differed (scenarios included, for example, an IT team and a



**Picture 1.** Scenario of communicative AI operating in a group chat.

marketing team). In the interviews, we made use of the screen share function on Zoom and Teams to share the scenario material with the informants. In practice, the section of the interview including the scenarios started with the interviewer explaining that the pictures the informant was going to see included an imagined group communication situation where a communicative AI was one of the participants. Then, the interviewer talked through the scenario, describing both what people and the communicative AI did. Finally, the interviewer asked the informant to reflect on what they had seen. Examples of specific questions in this section included ‘what kind of thoughts and feelings does the communicative AI’s actions raise in you?’, ‘would you hand over your own communication data for the training of this type of communicative AI?’, and ‘do you think knowledge about data collection would change the way people communicate in your organization?’

### *Data analysis*

We analyzed the data using iterative qualitative analysis (Tracy, 2020), which highlights a cyclical movement between empirical material and existing theoretical ideas related to the topic of the study. Our aim was to generate a rich thematic understanding of how the informants made sense of surveillance and privacy issues in relation to communicative AI in the workplace. In practice, during the first cycle of analysis, the first author engaged with the interview data by listening to the audio recordings and reading the transcriptions to get a well-rounded picture of *what* was in them. Here, the themes of surveillance and privacy served as conceptual starting points guiding attention to sections of the material where the informants talked specifically about, for example, data and its uses in the context of work, possible future use cases of communicative AI in their organization or their worries over employer surveillance catching their private lives. To keep track of the emerging observations, the first author wrote research memos, which, at this point, detailed different types of ‘risky data’ (that is, data informants saw as risky to hand over to a communicative AI) as well as two approaches to surveillance and privacy found among the informants: the detached and the emotional response. The final step of the first analysis cycle was a meeting between the team of authors to discuss these insights and to determine how the process should continue. It was here that, for example, Nissenbaum’s (2010) contextual integrity framework emerged as a potential theoretical device to approach the data.

In the second cycle, the first author engaged with the data through primary-cycle coding (Tracy, 2020: 219), that is, the coding was meant to capture basic level insights from the data in a systematic fashion. Guided by the study’s research question regarding how the informants approach privacy and surveillance in the context of organizational communicative AI, the initial codebook included codes for, for example, the different types of data considered as ‘risky’, informants’ reactions to being surveilled, perceived risks related to data collection, different emotional responses to privacy issues, and so on. While the insights from the initial round of listening provided a basis for the analysis, the first author kept an open approach to the material allowing new codes to emerge. After primary-cycle coding was completed, the final step of the analysis cycle was again a joint analysis meeting between the authors. Here, through interrogating the emerging codes, a sense of the prevalent second-level themes in the data started to emerge. Secondary-cycle coding involves the researcher critically examining the codes identified in primary cycles and further organizing, synthesizing and categorizing them into interpretative concepts or ‘second-level codes’ (Tracy, 2020: 225). This secondary-cycle analysis took place in the author team’s joint discussion, recorded in research memos.

Finally, in the third cycle of iteration, the insights developed in the analysis meeting during the second cycle were developed into the categorizations found in the Findings section of this study.

Essentially, the peer-debriefing practice (Lincoln and Guba, 1985) we used throughout the analysis process to collaboratively interrogate and refine the emerging analysis enabled us to identify the most prevalent approaches to privacy in the data – detached, compartmentalized, and affective – as well as to map the different data types identified in primary cycles meaningfully to these approaches. This final cycle leaned first more heavily into the empirical material in that the approaches are data-driven; however, they are analytically motivated by theoretical approaches to framing privacy as a social and contextual practice (Nissenbaum, 2010) rather than a legal and data-focused claim.

## **Findings: Knowledge workers' privacy concerns regarding communicative AI**

### *Detached approach to privacy: Distancing oneself from privacy concerns*

The first prevalent discourse that emerged throughout our interview data can best be described as a detached approach to privacy issues. This approach is twofold. First, several participants explained how they do not handle any sensitive data in their own work, so privacy issues did not really concern them personally. For example, Arthur (who works in IT-consulting) was asked what kinds of data he would be willing to share with a group-based communicative AI, and he immediately replied, 'Almost everything', and continued thinking about the different kinds of data he works with: 'Super confidential trade secrets and such, I don't deal with those in my work'.

This and similar comments reveal an approach to privacy, where privacy is diminished to denote data protection. The shared understanding regarding privacy in this approach is that there exist certain definable and clear data types that should be (and can be) protected. These data types included personal data, financial data, business and trade secrets, customer data, and data that fell under journalistic source protection. In this understanding of privacy, where it is seen as something that can be protected by controlling access to specific types of sensitive data, it is not a concern for employees who do not handle such data in their work. This line of reasoning can also lead to privacy issues being dismissed altogether as someone else's responsibility, as was suggested by Mike (who works in a media company):

"Well, I think that there are better people in our organization to make the assessment of whether there are risks or whether there is something ethically questionable about these tools." (Mike)

Second, many participants argued that as digital data are already everywhere, introducing group-based communicative AI to their workplace and giving it access to organizational data and team conversations would not change anything. Following this logic, Oliver (who works in regional development) ponders on how data management in its current state is not very well taken care of:

"Even now we have bits and pieces of data here and there, and people don't think about it. They don't worry if they have a post-it note on their table with some information on it for everyone to see. All data are so scattered anyway, how much would it hurt that the AI could access that data too." (Oliver)

This argumentation was also specifically connected to the digital infrastructure service provider that was used in the participants' respective organizations. Many reasoned that they already trusted certain service providers with their digital data, so why would they not trust them with this too. Jack (who works in a media company) explains this idea:

“On the other hand, all our data already live there on Microsoft’s servers. Since our company has decided that Microsoft can be trusted, wouldn’t it then be possible for us to trust that some bot like this could also work with that data.” (Jack)

Some participants also noted how their data in general was not that important or interesting, which led to thinking that privacy concerns did not really impact them:

“If a company like Microsoft somehow gets caught or starts misusing organizational data, then our organization is pretty much at the bottom of their list.” (Oliver)

In this detached approach to privacy, participants either saw that privacy related to certain clearly-defined data types that could be managed through controlling access to them, and, as they did not handle these data types in their work, privacy issues did not concern them; or, they considered privacy in many ways already lost and, as digital data were already everywhere, this new tool would not change the current situation in any meaningful way. The focus in this approach was on protecting specific types of data through system-level safeguards or clearly defined responsibilities, thus understanding privacy foremost as a legal and data-related issue and not as a social problem (Bennett, 2008). This was combined with reasoning resembling ‘digital resignation’, a condition where individuals would want to control how their digital data are collected and used but feel unable to do so (Draper and Turow, 2019). However, those participants who reasoned in this manner did not express any desire to change the situation but merely stated it as a fact.

### *Compartmentalized approach to privacy: Highlighting practical or administrative solutions*

The second approach to privacy implications of group-based communicative AI arising from our data set was to compartmentalize privacy-related reasoning as not relevant in the context of work. In this approach, the workplace was seen to exist only for working and consequently only work-related data were seen as being produced there. For example, Annie (who works in the chemical industry) explained how everything she does at work belongs to her employer, and that ‘*no personal matters are taken care of at work*’. Consequently, this approach included viewing all data produced at work as being the employer’s property. Similarly, Tammy (who works in education) explained:

“Whatever you do in your job and get paid to do, you do for your employer. [...] So can’t the organization then itself determine what it does with that data?” (Tammy)

Besides compartmentalizing work-related data as something owned by the employer, this approach also entailed participants engaging in practices of separating work-related and personal communication from each other. Many participants expressed how they refrain from communicating personal issues via organizational communication channels, and stated that as they did not communicate their personal issues at work or via employer’s communication channels, there was no need to think about privacy issues in this context. For example, Mike explained how he used the communication tools provided by his employer to send messages only on work-related issues: ‘*I don’t send messages in work channels that could somehow endanger my own reputation*’. Similarly, Annie had solved the need for communicating both work and personal issues by having two separate phones: ‘*I also like to keep work and home matters separate, I even have different phones for them*’.

This compartmentalizing of work and personal issues was at times also cemented in organizational policy and internal instructions on what can and should be communicated in different work-related communication channels. For example, Darlene (who works in education) described how employees in her organization were instructed on what should be shared in work-related communication channels:

“And we have certain policies as to how you can communicate in Teams and what you can’t write there, so there is no such [personal] information there.” (Darlene)

In this approach some participants also expressed a desire or a need to create clear communication policies for group-based communicative AI if it were introduced into their organization. This need connected particularly with the communicative AI’s suggested ability to add a new member to any chat group. That functionality raised concerns regarding pre-set communication channel structures and the social difficulties of removing someone from a channel when they had been added there. Such thoughts were presented by, for example, Thomas (who works in a media company):

“What if I’m talking with Laura on Y team’s channel and the bot comes there and realizes that there is a person in the organization’s Estonian subsidiary who knows about the issue we are talking about and brings that person into the conversation. That can break our agreed communication channels... Would we really want Estonia’s best expert on that matter to join our channel [...] and stay there permanently?” (Thomas)

Participants also raised content-related contextual challenges communicative AI could face, that would potentially infringe employees’ right to privacy. Jack, for example, worried the communicative AI would mix up personal details and work-related expertise when answering queries, and thus could inadvertently reveal personal information:

“Let’s say I want to find a journalist in the house who knows a lot about mental health problems. Will the AI point me toward a journalist who has written about that topic or a journalist who has often visited the occupational health psychologist?” (Jack)

The compartmentalized approach to privacy built on the view that at work employees (should) only produce and share work-related data, and that data belonged to the employer: As employees were operating within their employer’s organizational space and using equipment controlled by the employer, their right to privacy in this context was understood to be minimal (Kidwell and Sprague, 2009; Ravid et al., 2020). While participants considered their privacy rights in relation to work-related data to be minimal, they still worried about the privacy of their personal communications, which led them to compartmentalise their communication practices in very concrete manners (e.g. by using two phones).

The contextual integrity framework (Nissenbaum, 2010) can further shed light on these practices and privacy concerns. In the compartmentalized approach, many participants explained preserving their contextual integrity by restricting the types of information they shared (i.e. ‘attributes’). Participants’ privacy concerns related to the ‘contexts’ where information was shared and the ‘actors’ who participated in information sharing: They worried about the communicative AI’s role as an actor in their group discussions particularly when it came to its abilities (or rather, inabilities) to understand social contexts, as it might inadvertently reveal something (from another context) that was meant to be private. Thus, it was not only that the AI could act in certain contexts, but that it could mix contexts, which caused concern among the employees.

### *Affective approach to privacy: Focusing on the technology's surveillant functionalities*

The third approach that arose from our data describing how participants made sense of the privacy implications of communicative AI in a group setting is termed affective. The argumentation in this approach was less pragmatic and practical compared to the first two approaches, and more based on feelings (mostly of fear, insecurity, or anxiety) and concerns toward the technology's possible future developments. Several participants were strongly against implementing this kind of communicative AI into their workplace because they were concerned about the possible privacy infringements it might cause and because it was seen as an employee surveillance tool in a negative sense, or thought to have a trajectory to evolve into one. Participants who were insecure about using communicative AI in general spoke about their concerns relating to storing and using the data collected by AI. For example, Charlotte (who works in marketing) was asked what she thought would be the risks in implementing group-based communicative AI to her workplace, to which she responded:

“This might sound like I'm wearing a tinfoil hat... But, where is our data going to end up; how can 'it' be so frighteningly aware of things; and, now 'it' knows too much about us.” (Charlotte)

Henry (who works in education) described similar concerns when thinking about giving his own scientific text for communicative AI to comment on and to improve. In addition to not being able to know how his text would be used in the future, Henry worried about the ownership of ideas that he would develop together with communicative AI:

“Well, it kind of feels scary to me because of two things: A, where will the data go and how will it be used and then B, I would be afraid of the thought of not knowing exactly what my own thinking and my own ideas are.” (Henry)

While Henry and Charlotte were able to specify their concerns to some extent, there were many participants who merely intuitively did not want to be targeted by data collection in this manner. For example, Margaret (who works in research) expressed that she *'hasn't really thought about'* giving her data to communicative AI, but *'now that I do, I can't really give a rational argument about it, other than that it would feel bad or strange'*. Jasmin (who works in education) described similar feelings of unease:

“Artificial intelligence can be used for surveillance and monitoring too, we all know what has happened in China, for example. And my thoughts about this are quite negative [...] I'm quite a private person in many ways. So, if everything I type with my computer, whether it's my personal or work matters, would be used by some artificial intelligence... intuitively I get the feeling that it would not be okay.” (Jasmin)

Some participants relied on well-known symbols, such as 'Big Brother', referring to George Orwell's famous novel *1984*, or historical organizations known for their excessive surveillance practices, such as 'Stasi', referring to the state police in East Germany between 1950 and 1990, in explaining why they oppose this technology. David (who works in IT-consulting), for example, explained how communicative AI, such as the one suggested in the scenarios, would make him feel like he was being watched:

“I'd be scared if an AI tool could access my emails and one-on-one Slack messages, I'd get a feeling that Big Brother was watching me. [...] And I think that then I would move my conversations somewhere else.” (David)

Similarly, John (who works in a media company) worried about the surveillance potential of this technology and suspected that even if this kind of communicative AI was not intended for management to surveil employees, it would develop toward that direction:

“We journalists are all so cynical that if we were told that now your messages are being read by an AI tool [...], the first thought most of us would have is that ‘Okay, soon this technology will be used by the management to check who is working, and who is not.’ [...] My experience from the newsroom is that no one would want a general Stasi supervising us here.” (John)

Lastly, many were concerned about their private conversations. For example, Rose (who works in a media company) worried about her conversations being stored somewhere and analysed that when combined, they could reveal something essential about her: *‘I’m scared of the thought of some of my habits or my conversations being picked up, like a file, that would describe how I behave’*. Rose also worried about the social consequences of conversations leaking to unintended recipients:

“I would be worried that if I’d talk about something even a little bit outside of work in some chat group, then the bot would appear there and say something like ‘I have now made notes about this little gossip moment of yours and they can be found on the shared drive. I have also sent that memo directly to your boss and he has been invited to this meeting of yours which I have titled “Our boss messed up”.’ (Rose)

It is important to mention here that while many of the comments regarding the presumed surveillance capabilities of the technology were negative and several participants expressed their opposition toward surveillant uses, there were also numerous participants who did not have an affective response towards this technology and stated that they did not mind surveillance in this context. For example, Emma (who works in education) explained how she did not think about surveillance issues but focused on the possibilities this and similar technologies could offer:

“[When thinking about the risks of giving our data to a system like this] many people would probably mention data privacy and data security risks and such, but I don’t think about those issues, I think more about the possibilities [...] I’m so relaxed with my own data that I would probably give all possible information to the bot if it could help me with my tasks.” (Emma)

Emma described how she purposefully chose to dismiss any negative consequences the technology might introduce, making her overall approach more practical and convenience-oriented than affective. For her, risks related to ‘data privacy’ in general without further specification. Similarly, many participants who were more affective in their approach towards this technology and its privacy implications described concerns that were unspecified in nature. However, among those participants, there was a distinct concern that their employer would gain access to their communication data and use that information somehow to their disadvantage. These concerns, again, speak to the importance of evaluating who the ‘actors’ in information sharing are and how they affect informational norms (Nissenbaum, 2010), as the fear of privacy breaches connect to the range of actors and the possibility of information recipient not being what was expected or intended.

Overall, the affective approach was labelled by uncertainty and intuitive feelings of fear and dislike associated with unwanted leaks of personal and intimate data and the effect those leaks could have on social relationships. These negative feelings arose particularly in situations where data collection was seen as too detailed or not considered as necessary in the context of work (Ball, 2010), thus breaching participants’ expected levels of privacy.

## Discussion: Consequences to communication

The emerging literature on how communicative AI is used at work has thus far not focused on privacy and surveillance issues – rather, these viewpoints have been mentioned in passing or diminished to denote data protection when examining communicative AI in one-on-one settings. While no commercial communicative AI tools capable of interacting with a group of knowledge workers yet exist, their development is well under way given the collaborative nature of modern knowledge work and the possibilities of AI in enhancing it (see e.g. Houde et al., 2025). The scenarios in our interview protocol allowed us to explore knowledge workers' understandings of group-based communicative AI before it is widely adopted in organizations. Our findings illustrate how the adoption and use of communicative AI in a group at the workplace bring about specific considerations of privacy and surveillance.

While some privacy risks have been recognized in previous research, including concerns over data ownership, risks of external entities' attacks targeting communicative AI user data, and risks of inadvertently inputting personal data into the AI model (Das et al., 2025; Gupta et al., 2023), our study revealed novel risk-perceptions, many of which related to communicative AI operating within group conversations. For example, communicative AI's incapability to understand specific informational contexts raised concerns of possible privacy breaches, as the communicative AI could potentially share information in wrong contexts or to inappropriate recipients. Knowledge workers also worried that communicative AI's functionalities that supported data collection would render it to be used for surveillance purposes, either by management or by someone else, thus expanding the range of recipients of any information shared with the technology. A specific surveillance-related concern was that as communicative AI could collect the minutiae of peoples' everyday life from different sources, it could combine that data and use it to create a 'file' of a person, also conceptualised as a 'data double' (Haggerty and Ericson, 2000), that could be used in an unknown manner.

Many of the fears and risk-perceptions we recognized in this study connect to communicative AI's role as an actor in group discussions. In the contextual integrity framework (Nissenbaum, 2010), actors are one of the parameters characterizing context-relative informational norms. In our group chat scenarios, the actors who took part in the discussions included the employees (as the senders, recipients, and subjects of information) and the communicative AI (as the sender and recipient of information). When contemplating on the scenarios and the tasks suggested for the communicative AI to perform in the group chat, many participants expressed concerns that communicative AI itself would *act* in a manner that would lead to revealing inappropriate information in an inappropriate context to inappropriate recipients. It was the agentic properties of the technology – the fact that it had communicative agency to begin with (e.g. Sundar and Lee, 2022) – that turned into the focal point of concern. Consequently, participants' privacy concerns moved beyond issues relating to personal data control and connected more to how people in the organization relate to other people and how the communicative AI might in the future be able to change those relations. While previous research has shown that new technology (and specifically AI technology) can alter social relations in organizations (e.g.d Einola et al., 2024), it has not fully addressed the relational aspects of communicative AI. Consequently, our findings may be interpreted as part of a larger trend in seeing technology as a relational actor in organizations (Einola et al., 2024; Guzman and Lewis, 2020).

Furthermore, in terms of actors, we also recognized a distinct concern that employers could gain access to employees' communication data through group-based communicative AI, and would be able to surveil the employees or use their communication data somehow to the employees'

disadvantage. Due to these concerns, many participants predicted that a ‘chilling effect’ would take place were group-based communicative AI brought into their organization, referring to self-restraint and/or self-censorship that new surveillance-enabling digital technologies can produce (see e.g. [Manokha, 2018](#)). Furthermore, they foresaw how implementing this technology would drastically change communication practices in their organization: Employees would consider what they discuss, where, and how.

In addition to extending knowledge on specific surveillance-related fears employees have in relation to group-based communicative AI, our study contributes to the understanding of employee perspectives on and their approaches to privacy in the workplace. Building on our data, we recognized three distinct approaches knowledge workers had toward privacy risks in using group-based communicative AI at work. The first privacy approach could best be described as ‘detached’. Analyzing this approach adds to the study of ‘digital resignation’ ([Draper and Turow, 2019](#)), which recognizes how people want to control their own digital data but feel unable to do so. Our study brings nuance to the idea of resigning: for some individuals, resignation has developed to a point (or perhaps has always been so) where they do not even desire to prevent data spread, but rather accept it as a state of fact. This stance is qualitatively different from ‘resigning’, which entails feelings of helplessness or futility ([Draper and Turow, 2019](#)). Individuals who are detached from privacy simply accept that data are everywhere and rationalize this through, for example, statements of trust.

The second privacy approach we recognized was compartmentalizing privacy issues as something irrelevant in the context of work where no personal data was shared. This finding empirically elaborates [Nissenbaum’s \(2004, 2010\)](#) basic idea on the differences between social contexts and context-relevant informational norms, and demonstrates how even within a specific context (work) there can be distinct social contexts that are governed by different sets of rules and expectations for privacy. Some of the examples we introduced in our study illustrate concretely how individuals themselves separate different contexts via technological solutions and how they express a desire for clear communication policies to be implemented in regards to new technologies at the office.

The third privacy approach we recognized is termed affective. Most of the affective responses towards the idea of a group-based communicative AI in the workplace were negative, including feelings of fear, dislike, and uncertainty, and surveillant reasoning and logics were commonly used to make sense of the suggested technology and its privacy implications. The fears expressed by knowledge workers were directed towards the unknown possible future uses of this technology. Indeed, many expected a process of ‘surveillance creep’ to take place, where a technology intended for one purpose broadens beyond its original scope ([Haggerty and Ericson, 2005](#); [Innes, 2001](#)). Research on users of communicative AI has found that many who use this technology do not really know what the technology is able to do, the extent of what it can ‘know’, or is able to ‘learn’ ([Luger and Sellen, 2016](#)). Our study suggests that the uncertainty regarding the technology’s potential can cause fear which can lead to refraining from using the technology for certain tasks, or even altogether.

Overall, our findings demonstrate how communicative AI in a group setting in the workplace brings about specific approaches to privacy and distinct concerns relating to surveillance. While some employees distance themselves from privacy concerns and others compartmentalize privacy as not relevant in the work context, some express emotional responses to potential privacy infringements this technology and its surveillant functionalities might cause. The main privacy-related concerns among our participants were that the communicative AI would share employees’ private data with someone unauthorized (i.e. act in a manner that presented privacy risks), or that the data collected by the AI tool would be accessed by someone other than those participating in the

conversation (e.g. the employer). We have discussed these concerns through the actor parameter in the contextual integrity framework (Nissenbaum, 2010). As the framework itself does not consider technology as an actor, and as our empirical findings demonstrate that technology had a distinct role in potentially causing privacy conflicts, we suggest that the CI framework should be expanded to include the notion of technologies as actors, and future studies should explore the specific implications of this change. At the current stage of technological development, where artificial intelligence tools have greater autonomy than before and are able to carry out various tasks independently, the impact of their agency on user's privacy calls for continuing investigations.

## Conclusions

This research set out to analyse how knowledge workers approach and make sense of group-based communicative AI technology from privacy and surveillance viewpoints. Building on 33 qualitative interviews, we recognized three prevalent approaches to privacy: detached, compartmentalized, and affective. These approaches demonstrate how users' understanding of privacy issues relating to communicative AI expand mere data protection or data breaches to include concerns on how the technology could be used by the management for surveillance purposes, how the technology itself interacts within the organization, and how it will develop in the future. These findings are important, as the concerns we recognized have the potential to affect how employees want to use this technology in their own work. Thus, we suggest that for organizations to succeed in implementing communicative AI in the workplace (especially in the context of teamwork), they should consider employee privacy concerns presented here, as well as employees' affective responses to possible privacy risks and surveillant functionalities of this technology. Increasing transparency on how these technologies work (Das et al., 2025) and what data they collect, creating clear internal policies on their use, and advising users on how to make informed decisions about their usage (Feuerriegel et al., 2024; Gilmore et al., 2025; Gupta et al., 2023) would make communicative AI tools more ethically sound.

No study is without its limitations. Given that we used a prompt-led approach to elicit reactions and reflections from our informants regarding communicative AI in a group, the tentativeness of the findings needs to be acknowledged. In other words, while our informants were self-identified active users of communicative AI at work, their experience of it remained in the context of one-to-one conversation and they had no 'real' experience of conversing with a communicative AI in a group setting. Consequently, the design of the prompts used in the interview situation may have shaped the informants' responses in multiple ways: For example, the level of perceived agency the communicative AI had in each scenario could induce different types of responses, that is, it is qualitatively different to see a communicative AI suggesting an idea in a brainstorming situation (much like a commercial AI tool currently would) versus seeing it declare a time and place for a joint meeting it has already included in everyone's calendars. Nevertheless, the scenario-based interview method did allow us to explore a phenomenon that will possibly enter workplaces in the near future and to examine responses to it early on, while building ground for future, organizationally situated, studies.

Finally, we conclude by making two suggestions connected to the field of Surveillance Studies. Among surveillance scholars there is uncertainty as to how communicative AI will change surveillance: Will it merely increase the already vast possibilities for different kinds of digital surveillance, or is there something meaningfully new in its operations? We argue for the latter approach. Communicative AI tools are distinct from other data collection tools as they operate autonomously and, by definition, they are intelligent: communicative AI has the ability to connect bits and pieces of

data, create something more from it, and share those findings independently. These functionalities cause alarm in the users and, from a surveillance perspective, are meaningfully new: The idea that a technology is able to not only read, but understand, connect, and implement the knowledge it collects adds to previous understanding of surveillance technologies' expected capabilities, and, as demonstrated in our study, raises many ethical and privacy-related concerns in the users. Furthermore, communicative AI tools differ from other employee surveillance tools in that they make the infrastructural data collection visible, and this visibility is highlighted in situations where communicative AI reveals something it should not have revealed, in other words, when it makes a mistake. As these situations are also profoundly humane, they highlight the human-like nature of communicative AI, thus making it affectively different than other surveillance technologies, and highlighting the importance of continuing research on its privacy implications.

### **Author's note**

Koivula and Leppälä conducted this research at the University of Helsinki. Koivula's current affiliation is at the Department of Language and Communication Studies, University of Jyväskylä, and Leppälä's at the Department of Information and Knowledge Management, Tampere University.

### **Acknowledgements**

We would like to thank the SODA and GET:ORG project teams for support and feedback on earlier versions of this manuscript. Additionally, our thanks go to Salla-Maaria Laaksonen for her help in data collection and Vilma Karjalainen for assisting with the interview transcripts as well as our participants for their time.

### **ORCID iDs**

Liisa A. Mäkinen  <https://orcid.org/0000-0001-6141-503X>

Minna Koivula  <https://orcid.org/0000-0002-7718-0199>

Mia Leppälä  <https://orcid.org/0009-0000-5209-5409>

### **Ethical considerations**

No institutional ethical approval was required for this study.

### **Consent to participate**

Participation in this study was voluntary. All participants were informed of their rights and informed consent to participate was collected in written form.

### **Consent for publication**

All participants signed written informed consent forms allowing for the research to be published.

### **Funding**

The authors disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work was supported by the Foundation for Economic Education.

### **Declaration of conflicting interests**

The authors declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

## Data Availability Statement

No data from this study is publicly available.

## References

- Altman I (1976) Privacy. A conceptual analysis. *Environment and Behavior* 8(1): 7–29.
- Ball K (2002) Editorial. The labours of surveillance. *Surveillance and Society* 1(2): 125–137.
- Ball K (2010) Workplace surveillance: an overview. *Labor History* 51(1): 87–106.
- Ball K (2021) *Electronic Monitoring and Surveillance in the Workplace. Literature Review and Policy Recommendations*. Publications Office of the European Union.
- Ball K (2022) Surveillance in the workplace: past, present and future. *Surveillance and Society* 20(4): 455–461.
- Barnes SB (2006) A privacy paradox: social networking in the United States. *First Monday* 11(9). Available at: <https://doi.org/10.5210/fm.v11i9.1394>
- Bennett CJ (2008) *The Privacy Advocates. Resisting the Spread of Surveillance*. The MIT Press.
- Brynjolfsson E, Li D and Raymond L (2025) Generative AI at work. *Quarterly Journal of Economics* 140(2): 889–942.
- Cousineau LS, Ollier-Malaterre A and Parent-Rocheleau X (2023) Employee surveillance technologies: prevalence, classification, and invasiveness. *Surveillance and Society* 21(4): 447–468.
- Das BC, Amini MH and Wu Y (2025) Security and privacy challenges of large language models: a survey. *ACM Computing Surveys* 57(6): 1–39.
- Degli Esposti S (2014) When big data meets dataveillance: the hidden side of analytics. *Surveillance and Society* 12(2): 209–225.
- Draper NA and Turow J (2019) The corporate cultivation of digital resignation. *New Media & Society* 21(8): 1824–1839.
- Einola K, Khoreva V and Tienari J (2024) A colleague named max: a critical inquiry into affects when an anthropomorphised AI (ro)bot enters the workplace. *Human Relations* 77(11): 1620–1649.
- Feuerriegel S, Hartmann J, Janiesch C, et al. (2024) Generative AI. *Business & Information Systems Engineering* 66(1): 111–126.
- Gilmore JN, Whims T, Blair BW, et al. (2025) Technology acceptance, moral panic, and perceived ease of use: negotiating ChatGPT at research one universities. *Convergence: The International Journal of Research into New Media Technologies* 31(4): 1251–1266.
- Gkinko L and Elbanna A (2022) Hope, tolerance and empathy: employees' emotions when using an AI-enabled chatbot in a digitalised workplace. *Information Technology & People* 35(6): 1–11.
- Gupta M, Akiri C, Aryal K, et al. (2023) From ChatGPT to ThreatGPT: impact of generative ai in cybersecurity and privacy. *IEEE Access* 11: 80218–80245.
- Guzman AL and Lewis SC (2020) Artificial intelligence and communication: a human–machine communication research agenda. *New Media & Society* 22(1): 70–86.
- Haggerty KD and Ericson RV (2000) The surveillance assemblage. *British Journal of Sociology* 51(4): 605–622.
- Haggerty KD and Ericson RV (2005) The new politics of surveillance and visibility. In: Haggerty KD and Ericson RV (eds) *The New Politics of Surveillance and Visibility*. University of Toronto Press, 3–25.
- Heiselberg L and Stepińska A (2022) Transforming qualitative interviewing techniques for video conferencing platforms. *Digital Journalism* 11(7): 1353–1364.
- Heuser M and Vulpius J (2024) Grandma, tell that story about how to make napalm again?: exploring early adopters' collaborative domestication of generative AI. *Convergence: The International Journal of Research into New Media Technologies*, Epub ahead of print 26 September 2024. DOI: [10.1177/13548565241285742](https://doi.org/10.1177/13548565241285742).

- Houde S, Brimijoin K, Muller M, et al. (2025) Controlling AI agent participation in group conversations: a human-centered approach. In: Li T, Paternò F, Väänänen K, et al. (eds) IUI '25: Proceedings of the 30th International Conference on Intelligent User Interfaces. Cagliari, Italy, 24–27 March 2025, 390–408.
- Innes M (2001) Control creep. *Sociological Research Online* 6(3): 13–18.
- Jarrahi MH (2018) Artificial intelligence and the future of work: Human-AI symbiosis in organizational decision making. *Business Horizons* 61(4): 577–586.
- Jiménez TR and Orozco M (2021) Prompts, not questions: four techniques for crafting better interview protocols. *Qualitative Sociology* 44: 507–528.
- Kidwell RE and Sprague R (2009) Electronic surveillance in the global workplace: laws, ethics, research and practice. *New Technology, Work and Employment* 24(2): 194–208.
- Kieslich K, Diakopoulos N and Helberger N (2024) Using scenario-writing for Identifying and mitigating impacts of generative AI. arXiv preprint arXiv:2410.23704.
- Lincoln YS and Guba EG (1985) *Naturalistic Inquiry*. Sage.
- Lucia B, Vetter M and Patel V (2025) The dystopian imaginaries of ChatGPT: a designed cycle of fear. *Convergence: The International Journal of Research into New Media Technologies*, Epub ahead of print 18 April 2025. DOI: [10.1177/13548565251333212](https://doi.org/10.1177/13548565251333212).
- Luger E and Sellen A (2016) “Like having a really bad PA”: the gulf between user expectation and experience of conversational agents. In: Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, San Jose, CA, 7–12 May 2016, pp. 5286–5297.
- Mahnke MS (2024) Taming’ generative AI at work: balancing technological promise with professional values. *Southeast Asian Media Studies Journal* 6(1): 33–46.
- Mahnke MS and Bagger C (2024) Navigating platformized generative AI: examining early adopters’ experiences through the lens of data reflectivity. *Convergence: The International Journal of Research into New Media Technologies* 30(6): 1974–1991.
- Manokha I (2018) Surveillance, panopticism, and self-discipline in the digital age. *Surveillance and Society* 16(2): 219–237.
- Mayer-Schönberger V and Cukier K (2013) *Big Data: A Revolution that will Transform How We Live, Work, and Think*. Houghton Mifflin Harcourt.
- Mettler T (2024) The connected workplace: characteristics and social consequences of work surveillance in the age of datification, sensorization, and artificial intelligence. *Journal of Information Technology* 39(3): 547–567.
- Nissenbaum H (2004) Privacy as contextual integrity. *Washington Law Review* 79(1): 119–157.
- Nissenbaum H (2010) *Privacy in Context: Technology, Policy, and Integrity of Social Life*. Stanford University Press.
- Nissenbaum H (2015) Respecting context to protect privacy: why meaning matters. *Science and Engineering Ethics* 24(3): 831–852.
- Raisch S and Krakowski S (2021) Artificial intelligence and management: the automation–augmentation paradox. *Academy of Management Review* 46(1): 192–210.
- Ramaul L, Ritala P and Ruokonen M (2024) Creational and conversational AI affordances: how the new breed of chatbots are revolutionizing the knowledge industries. *Business Horizons* 67(5): 615–627.
- Ravid DM, Tomczak DL, White J, et al. (2020) EPM 20/20: a review, framework and research agenda for electronic performance monitoring. *Journal of Management* 46(1): 100–126.
- Sergeeva AV, Faraj S and Huysman M (2020) Losing touch: an embodiment perspective on coordination in robotic surgery. *Organization Science* 31(5): 1053–1071.
- Söllner M, Arnold T, Benlian A, et al. (2025) ChatGPT and beyond: exploring the responsible use of generative AI in the workplace: an interdisciplinary perspective. *Business & Information Systems Engineering* 67: 289–303.

- Stanton JM (2003) Information technology and privacy: a boundary management perspective. In: Clarke S, Coakes E, Hunter GM, et al. (eds) *Socio-Technical and Human Cognition Elements of Information Systems*. IGI Global, 79–103.
- Stanton JM and Stam KR (2003) Information technology, privacy, and power within organizations: a view from boundary theory and social exchange perspectives. *Surveillance and Society* 1(2): 152–190.
- Sundar SS and Lee E (2022) Rethinking communication in the era of artificial intelligence. *Human Communication Research* 48(3): 379–385.
- Tang KS (2024) Informing research on generative artificial intelligence from a language and literacy perspective: a meta-synthesis of studies in science education. *Science Education* 108(5): 1329–1355.
- Tracy SJ (2020) *Qualitative Research Methods: Collecting Evidence, Crafting Analysis, Communicating Impact*. 2nd edition. Wiley-Blackwell.
- van Dijck J (2014) Datafication, dataism and dataveillance: big data between scientific paradigm and ideology. *Surveillance and Society* 12(2): 197–208.
- Westin A (1967) *Privacy and Freedom*. Atheneum Press.