Communications of the Association for Information Systems

Volume 55 Paper 23

10-8-2024

Watch Out, You are Live! Toward Understanding the Impact of AI on Privacy of Employees

Ashneet Kaur
SP Jain Institute of Management and Research, Mumbai, India, ashneet.kaur@spjimr.org

Sudhanshu Maheshwari
SP Jain Institute of Management and Research, Mumbai, India, sudhanshu.maheshwari@spjimr.org

Indranil Bose
NEOMA Business School, Reims, France, indranil_bose@yahoo.com

Simarjeet Singh
Great Lakes Institute of Management, Gurgaon, India, simarjeet.s@greatlakes.edu.in

Recommended Citation
Kaur, A., Maheshwari, S., Bose, I., & Singh, S. (2024). Watch Out, You are Live! Toward Understanding the Impact of AI on Privacy of Employees. Communications of the Association for Information Systems, 55, 603-626. https://doi.org/10.17705/1CAIS.05523

Watch Out, You are Live! Toward Understanding the Impact of AI on Privacy of Employees

Cover Page Footnote

This manuscript underwent editorial review. It was received 01/22/2024 and was with the authors for six months for two revisions. The Associate Editor chose to remain anonymous.

Communications of the Association for Information Systems

Research Article DOI: 10.17705/1CAIS.05523 ISSN: 1529-3181

Watch Out, You are Live! Toward Understanding the Impact of AI on Privacy of Employees

Ashneet Kaur
SP Jain Institute of Management and Research
Mumbai, India
ashneet.kaur@spjimr.org
0000-0002-6417-2122

Sudhanshu Maheshwari
SP Jain Institute of Management and Research
Mumbai, India
sudhanshu.maheshwari@spjimr.org
0000-0002-0288-1783

Indranil Bose
NEOMA Business School
Reims, France
indranil_bose@yahoo.com
0000-0002-5737-966X

Simarjeet Singh
Great Lakes Institute of Management
Gurgaon, India
simarjeet.s@greatlakes.edu.in
0000-0003-3497-2177

Abstract:

The rapid integration of Artificial Intelligence (AI) across diverse sectors, particularly in the workplace, has yielded efficiency gains and enhanced decision-making capabilities. However, the pervasive adoption of AI has raised significant concerns regarding the privacy of employees. This systematic literature review seeks to comprehensively explore the implications of AI on employee privacy. The study addresses three key dimensions: (1) evaluating the extent to which AI technologies compromise or safeguard employee privacy; (2) elucidating the costs and benefits of AI adoption in organizations to strike a balance with employee privacy considerations; and (3) discussing the varying impact of advancing AI algorithms in the workplace on employee privacy. Drawing upon the privacy calculus framework, the paper underscores the trade-offs organizations make in managing employees' privacy in the context of AI integration. The discussion is grounded in an analysis of advancing AI algorithms and their dynamic influence on the delicate balance between organizational efficiency and the protection of employee privacy. By addressing the complexities inherent in this intersection, the research serves as a valuable resource for guiding further inquiry into the evolving relationship between advancing AI technologies and preserving employee privacy.

Keywords: Artificial Intelligence, Privacy Calculus, Systematic Review, Employee Privacy.

This manuscript underwent editorial review. It was received 01/22/2024 and was with the authors for six months for two revisions. The Associate Editor chose to remain anonymous.

1 Introduction

"I feel like I'm being watched all the time. It's stressful knowing every keystroke is monitored." Another employee mentioned, "The idea that my employer can track my movements and analyze my behavior without my consent is deeply unsettling." These statements of employees published in the Pew Research Center report (Faverio & Tyson, 2023; Rainie et al., 2022) highlight a growing anxiety among employees about the pervasive use of AI surveillance in the workplace. The rapid integration of Artificial Intelligence (AI) across diverse sectors, particularly in the workplace, has yielded efficiency gains and enhanced decision-making capabilities. However, this pervasive adoption of AI has raised significant concerns regarding the privacy of employees.

In recent years, in the last decade, the rapid pace of technological advancement has significantly reshaped the business landscape (Cascio & Montealegre, 2016). This era is marked by an unprecedented acceleration in computational capabilities, with computational power reported to double approximately every 3.4 months, drastically enhancing the capabilities of AI across various sectors (Hao, 2019). By 2025, AI is projected to undertake 30% of global corporate audits, highlighting its growing role in everyday business functions (World Economic Forum, 2016; McStay, 2020). AI's influence extends beyond mere automation and efficiency and profoundly impacts how organizations manage and interact with their workforce. It represents a pivotal shift in the workforce management paradigm, where algorithmic management practices aim to transcend human limitations by augmenting intellectual and physical capacities through the adoption of AI-based systems in organizational settings (Cram & Wiener, 2020; Jain et al., 2021; Wiener et al., 2023). These systems, evolving from simple task performers to complex decision-makers, promise a synergy where human and machine intelligence coalesce to enhance productivity and decision-making processes (Benbya et al., 2021; Giermindl et al., 2022).

AI's integration into organizational ecosystems brings numerous benefits, yet its extension into employees' personal domains raises significant privacy concerns. Cardon et al. (2023) executed a sentiment analysis of employees, where employees revealed their discomfort with AI-based evaluation tools as such tools strip away the minimal existing privacy. The capacity of AI to analyze detailed human behaviours and interactions introduces scenarios where surveillance can become overly intrusive, potentially leading to the misuse of employee data (Mikhaeil & James, 2023; Markus, 2017). For instance, AI-driven tools like the "WorkSmart" platform by Crossover, a smart-employment movement tracking system, or the "FlowLight" system from a Swedish startup, which tracks employees through colored LEDs based on real-time activity monitoring or "Silent Watch" that provides employers with data on every keystroke made by employees, indicate a trend where employee monitoring tends to infringe on personal space and privacy (Goyal, 2018; Züger et al., 2017), raising critical questions about the balance between oversight and overreach. Considering the invasive nature of AI systems in the workplace, regulatory bodies worldwide are beginning to respond to these intrusive systems employed by organizations (Glasser & Forman, 2020). Hence, as AI continues to integrate across various organizational functions, the dual-edged nature of AI in business, while offering substantial benefits, requires careful management to protect employee privacy to avoid legal ramifications. This paper uses the privacy calculus framework, defined as a cost-benefit analysis, where information would be disclosed if the perceived benefits outweighed the associated risks (Culnan & Armstrong, 1999), examining the balance organizations must strike between safeguarding employee privacy and leveraging AI's potential.

Despite the critical importance of addressing the privacy implications of such developments (Jain et al., 2021), there remains a noticeable gap in the literature in the context of privacy concerns of employees related to AI adoption in the organization (Giermindl et al., 2022). This review aims to address this deficit by systematically examining the existing body of work on AI and privacy within the information systems (IS) field, offering a detailed exploration of how AI impacts employee privacy using a privacy calculus model. Our study utilizes an integrative literature review (Templier & Paré, 2015) to analyse the existing scholarly work on the AI-employee privacy domain. This method is especially relevant in fields where research is fragmented across diverse domains without a cohesive integration or comprehensive analysis by scholars (Scully-Russ & Torraco, 2020).

In the context of AI and employee privacy, the current literature predominantly consists of systematic reviews with a narrow focus on specific AI applications within organizational settings (e.g., Enholm et al., 2022; Heyder et al., 2023; Mikhaeil & James, 2023; Marabelli & Newell, 2023; Sewak et al., 2021). While valuable, these studies often lack a holistic view and do not construct a robust theoretical framework that

adequately addresses the broad implications of AI on employee privacy. Our review uniquely addresses this gap by systematically compiling and analyzing literature that spans multiple dimensions of AI applications and their privacy implications, providing a broader perspective that has been largely absent in current research. Furthermore, most existing studies lack a robust theoretical framework integrating advancing AI technologies with the complex dynamics of employee privacy (Benbya et al., 2021; Jain et al., 2021). Our work contributes significantly to this area by developing an overarching framework synthesizing existing findings and guiding future research on the intersection of AI and privacy. This framework particularly emphasizes the privacy calculus within organizational settings, which has not been comprehensively addressed in previous reviews. Additionally, our review is designed to be of practical use not just to academics but also to industry practitioners. By detailing specific implications for managing privacy concerns in light of AI advancements, our review serves as a valuable resource for those tasked with implementing and managing AI technologies in sensitive human-centric environments. This dual focus on theoretical development and practical application ensures that our research provides actionable insights and guidance, making it an essential reference for both scholarly inquiry and practical implementation.

Our comprehensive review thus identifies key themes and constructs a robust profile of current research at the nexus of AI and employee privacy. Through this enhanced comprehension, we formulate specific research questions to guide further inquiry, ensuring a thorough exploration of this critical area.

RQ1: What is the current status of the research profile in the existing literature on the intersection of AI and employee privacy?

RQ2: What are the research gaps and recommendations for scholars and practitioners in the context of future research on the implications of AI for employee privacy?

To address these research questions, our integrative review on the theme of AI and employee privacy will comprehensively examine both empirical and theoretical research conducted on this subject over the past two decades in the IS journals dating back to 2000. Despite the term "AI and employee privacy" not gaining widespread recognition until recent years, we have diligently accounted for potential publication lags and conducted a thorough literature search across leading databases for peer-reviewed articles. In response to RQ1, the first part of our review identifies, synthesizes, and presents a contemporary profile of the existing literature on AI and employee privacy. This encompasses an analysis of annual publication trends, coverage of studies and frameworks, and variables and measures related to the characterization and evolution of the topic. For RQ2, the second part of our review focuses on delineating the accumulated relevant research on AI and employee privacy from its inception to the present day. We described research findings published in literature over the past two decades, presenting details from selected articles in peer-reviewed journals during this timeframe to highlight gaps in the extant literature.

Building on these insights, we present potential avenues for future research and propose a state-of-the-art framework for advancing research on the implications of AI for employee privacy. The structure of the paper includes a brief background on the theme, a profile of existing literature, a description of the methodological process used in the integrative review, an enumeration of key aspects discussed in the literature, identification of gaps, formulation of future research themes, and recommendations. The paper concludes with a comprehensive discussion of the study's theoretical and practical implications and an acknowledgement of its limitations.

2 Conceptual Foundation

2.1 Artificial Intelligence

AI is traditionally seen as a system capable of processing external data, understanding it, and using this understanding to act in ways like human thought processes. This approach aims to match or even exceed human intelligence in specific tasks (Kaplan & Haenlein, 2019). Unlike simpler technologies that follow fixed instructions, AI can learn from the data it encounters. This learning capability means AI can change its actions over time without the requirement of reprogramming (Syam & Sharma, 2018). Because of this, organizations are increasingly using AI in tandem with human intelligence to achieve better results.

Researchers have explored various ways to classify AI. One approach by Kaplan and Haenlein (2019) divides AI into stages based on its complexity and processing capabilities: from basic, called artificial narrow intelligence, to intermediate, known as artificial general intelligence, and finally advanced, termed

artificial superintelligence. They also looked at AI through its functions: analytical tasks, those inspired by humans, and those more human-like. In a related effort, Giermindl et al. (2022) grouped AI into four categories based on the maturity level of AI algorithms: descriptive, predictive, prescriptive, and autonomous. Though there are many types of categorizations, this sub-type is comprehensive, effectively distinguishing between the nature of the technology and its application within organizational settings.

Descriptive AI involves algorithms that examine past events and their influence on the present (Wiener et al., 2023). For example, an organization may use such AI to analyze historical sales data to identify trends that inform stock management decisions. Predictive AI algorithms predict future developments by analyzing past or real-time data and assigning probabilities to different scenarios (Bauer & Gill, 2023). A practical application of predictive AI could be in the healthcare sector, where algorithms predict patient risks based on their health records and ongoing treatment responses. On the other hand, prescriptive AI uses advanced statistics, scenarios, and machine learning techniques to automatically generate decision recommendations (Marabelli et al., 2021). In the field of logistics, prescriptive AI might suggest the best routes for delivery drivers based on traffic conditions, weather, and delivery windows. Further, autonomous AI algorithms autonomously derive complex decisions, execute them, and communicate them based on self-learning processes, including learning from emotions (Mullins et al., 2022). This type of AI can be seen in vehicles that navigate traffic and adjust routes in real-time without human intervention. Drawing from these categorizations, our systematic review provides a framework that views varying AI in relation to employee privacy as machines designed to mimic human intelligence in performing tasks ranging from basic to autonomous functioning.

2.2 Employee Privacy and Privacy Calculus

The IS literature underscores the invasive nature of AI in the realm of people management, highlighting significant privacy concerns (Hamilton & Sodeman, 2020; Schlagwein & Willcocks, 2023; Simbeck, 2019). While the focus has traditionally been on the implications of AI applications for consumer privacy (Günther et al., 2017), there is a growing acknowledgement of its impact on employees as well. Privacy, as outlined by Simms (1994), pertains to the extent of external access to an individual's personal details, intimate life experiences, and innermost reflections. In a similar vein, employee privacy is understood as the employer's agreed-upon and restricted insight into the physical, intimate, or cognitive facets of their staff members (Ball et al., 2012). Yet, the escalating integration of advanced AI within organizational frameworks has obscured this delineation of privacy. This obscurity stems from AI's continually changing nature and growing capacity for intricate oversight, perpetually challenging an employee's expectation of a secure and private work environment. Such challenges often result in heightened employee unease and apprehension (Zhang et al., 2022). While earlier studies have touched upon the overarching merits and drawbacks of AI (Heyder et al., 2023; Markus, 2017), there's a pressing call to probe deeper into the effects of AI on employees' privacy (Jain et al., 2021; Nyman et al., 2023; Polyviou et al., 2023). Additionally, the strategic use of advancing AI in management practices remains notably sparse in current scholarly debates (Brynjolfsson & Mcafee, 2017). Algorithmic mechanisms, underpinned by rational controls, oversee workers' actions and, at times, may infringe upon their privacy (Zhang et al., 2022). Considering the above implications of AI on employee privacy and limited understanding in the scholarly literature, reconciling comprehensive cost-benefit dynamics of integrating AI from the privacy calculus framework becomes pertinent and requires further investigation.

The privacy calculus refers to a deliberate thought process wherein individuals weigh potential risks or costs against the perceived advantages linked to divulging personal data (Mikhaeil & James, 2023). The concept of privacy calculus emerges from foundational research in privacy that introduces a “calculus of behavior” (Laufer & Wolfe, 1977). In this framework, individuals are seen as trading a measure of privacy for some economic or social benefit based on their ability to manage any future consequences of their decisions in the present. For example, a cost-benefit analysis of employees can be used to determine the outcomes of providing personal information to organizations (Culnan & Bies, 2003; Bhave et al., 2020). This approach has remained a popular conceptualization within the literature (e.g., Mikhaeil & James, 2023; Bélanger & James, 2020). Further, Laufer and Wolfe (1977) have identified three pivotal elements that might unsettle this balance between cost and benefit: (1) entities might downplay the potential ramifications of sharing data, especially when a valuable benefit is associated with the revelation; (2) predicting the repercussions of such disclosures might be challenging; and (3) the emergence of innovative technologies can shift the outcomes of such data sharing.

With the advent of technologies capable of extracting micro-level information from users (Mikhaeil & James, 2023), such as AI, the privacy-calculus framework holds prominence for analyzing how employees weigh the costs of providing both work-related and personal information against the benefits that accrue to them from such disclosures through AI.

The instrumentality of the privacy-calculus framework can be further explained in the context of AI. The adoption of AI benefits the employees through accurate performance assessments but at the cost of compromised privacy as these technologies pose risks of excessive personal information disclosure, such as health details or personal messages, potentially beyond what is necessary for employers' access (Gal et al., 2020). Therefore, while such data extraction can facilitate robust managerial decision-making, it raises crucial concerns about how much decision-making compromises employee privacy (Mettler, 2023), especially in the context of the varying nature of AI capabilities.

Considering such discussions on privacy concerns due to changing technologies in the workplace, our research explores the evolving nature of AI technologies, which vary from descriptive to autonomous, each possessing different capabilities for extracting and analyzing user data. This study reviews the existing literature to identify gaps regarding AI and privacy and expands the discussion by examining how incremental AI capabilities affect the privacy calculus in organizational settings. Specifically, how these varying capabilities of AI influence the balance of costs and benefits for employees, affecting their privacy assessments and the overall dynamics within the workplace.

3 Methodology

Integrative reviews present a significant opportunity to comprehensively assess the current state of knowledge on a specific topic, catalyzing subsequent research endeavors (Torraco, 2016). Additionally, these reviews enable the generation of novel perspectives that may not have been previously explored in the existing literature. Importantly, they have the potential to exert a substantial influence on shaping both practical applications and the future trajectories of the field (Okoli, 2015). Hence, we have utilized a systematic literature review method in our study.

3.1 The Review Process

The review process consisted of six distinct stages, aligning with the established methodology for systematic literature reviews to ensure comprehensive coverage of the relevant literature (Enholm et al., 2022). Initially, a review protocol was developed, specifying the keywords and phrases chosen for the study. Subsequently, the search strategy and inclusion and exclusion criteria were established to identify the publications relevant to our review. The third stage involved searching for papers using predefined keyword combinations. Critical assessments were conducted on the articles retrieved during the search, followed by data extraction and synthesis of the findings. Further elaboration on these stages is provided in the subsequent subsections (see Figure 1).

3.1.1 Protocol Development

The systematic exploration of the literature was initiated by formulating a review protocol, meticulously crafted following the method elucidated in the *Cochrane Handbook for Systematic Reviews of Interventions* (Higgins, 2008). Within this protocol, the fundamental research queries were formulated concurrently with the strategic orchestration of the quest methodology, precise delineation of criteria for inclusion and exclusion, and the rigorous imposition of quality standards. Furthermore, the protocol explicitly dictated the chosen method for synthesizing the collected data. These inquiries that steered the review process were discreetly characterized as follows: What circumstances engender or encumber the adoption of AI within organizations? Through what mechanism does AI influence stakeholders' privacy? How does AI adoption have implications for employee privacy calculus? These research questions were the foundation for guiding subsequent steps, including selecting appropriate sets of keywords and data sources.

3.1.2 Inclusion and Exclusion Criteria

The systematic literature review incorporated a set of rigorously defined inclusion and exclusion criteria to delineate its boundaries. The inclusion criteria encompassed studies with a primary focus on elucidating the potential of AI on privacy or investigating AI's adoption and utilization within organizational contexts. Studies emphasizing the technical dimensions of AI, such as its infrastructural aspects or the comparative

analysis of distinct models, fell beyond the purview of the selected papers. No temporal boundary was set in terms of years. Hence, the search results comprised results across years. However, it was noted that primary results comprised research papers after 2010, emphasizing the wealth of innovative and novel AI applications that materialized within the last decade. Language restriction constituted an additional criterion, as only publications in the English language were considered within this review. This criterion ensured linguistic accessibility and effective comprehension for a wider readership. The systematic literature review granted exclusive attention to peer-reviewed publications, notably journal articles and conference proceedings. These publication types aligned best with scholarly rigor and peer scrutiny. Conversely, categories of publications such as book series, dissertations, reports, and web-based content were systematically excluded. This selective approach sought to maintain the elevated academic discourse and reliability standards throughout the review process.

3.1.3 Data Sources and Search Strategy

The initial step in our search strategy involved formulating search strings, and two distinct sets of keywords were curated. The first set comprised keywords pertinent to AI and its affiliated technologies, while the second set was constructed to encapsulate privacy and its related terms, secrecy, confidentiality, or solitude. Subsequently, these keyword sets were amalgamated, allowing the use of Boolean and proximity operators to streamline the search process. These concatenated search terms were then employed in each of the thirteen primary information systems journals, comprising *Information System Frontier*, *Decision Support Systems*, *European Journal of Information Systems*, *Information & Management*, *Information and Organization*, *Information Systems Journal*, *Information Systems Research*, *Journal of the Association for Information Systems*, *Journal of Information Technology*, *Journal of MIS*, *Journal of Strategic Information Systems*, *MIS Quarterly,* and *Communications of the Association for Information Systems*, using the electronic databases, encompassing, Scopus, Emerald, Taylor and Francis, Springer, Web of Science, ABI/Inform Complete, IEEE Xplore, and the Association for Information Systems (AIS) eLibrary. This comprehensive approach aimed to ensure the exhaustive inclusion of all pertinent articles in our review. The data collection initiative was initiated on August 15, 2023, and was finalized on September 15, 2023.

3.2 Data Filtration

3.2.1 Quality Assessment

Following the initial eligibility check, one of the co-authors extracted the whole data. Two other co-authors independently assessed the selected papers comprehensively. Their evaluation encompassed various criteria, including scientific rigor, credibility, and relevance. Scientific rigor pertains to applying an appropriate research methodology within the studies. Credibility focuses on the overall believability of the research and the effectiveness with which the findings are presented. Lastly, relevance gauges the extent to which the findings are pertinent to the academic community and organizations involved in AI initiatives. This multifaceted evaluation aimed to ensure that the remaining papers would offer substantial value to the review. Subsequent to this assessment, 81 papers were retained for the subsequent data extraction and synthesis phases.

3.2.2 Data Extraction and Synthesis of Findings

To facilitate the synthesis of findings, we constructed a concept matrix. This matrix served as an organizational tool to categorize the selected studies. It involved meticulously examining the papers, with the gathered information systematically structured within a spreadsheet. This method enhanced our capacity to draw comparisons across studies and elevate their findings to higher-level interpretations. The studies were scrutinized about the following focal areas: the adoption and utilization of AI in an organizational context, and the link of AI and its related technologies in privacy. Further, the screening of the papers corresponding to employee privacy was determined. In the matrix, we recorded essential information, including research methodology, pertinent definitions, the scope of analysis, key findings, employed theories, the investigative context, and other noteworthy concepts from each paper. To eliminate any possibility of selection and screening bias, the entire literature screening and selection process was conducted by two authors separately. The high value of the inter-rater reliability score (kappa= 0.87) ensures the consistency and reliability of the overall methodological process. Further, in the case of disagreement on selecting any research study, the authors reached a final decision through mutual consent. Subsequently, through an iterative approach, all co-authors collaboratively reached a

consensus regarding categorizing contexts and incorporating additional dimensions required to capture pertinent data comprehensively. Each of the remaining 55 papers was systematically analyzed and integrated into the concept matrix, paving the way for the subsequent synthesis of findings in Figure 1.

4 Synthesis of a Growing Body of AI-privacy Literature

4.1 Key Findings from the Review of Existing Literature

The last two decades have witnessed a transformative journey in IS research, focusing on diverse aspects ranging from effective AI systems to the intrusive nature of technology having economic implications, ethical concerns, and societal impacts.

Our review includes studies that probe the intersection of AI with human decision-making and organizational efficiency. For example, several debates have been arranged on the ratification of balancing algorithmic technology with human intelligence, which impacts decision-making processes (Lyytinen & Grover, 2017; Markus, 2017). These discussions are linked directly to economic outcomes as they influence organizations' strategies to maximize efficiency and minimize costs. Additional research has enriched our understanding of how AI technologies specifically affect economic aspects within organizations (Benbya et al., 2021; Enholm et al., 2022). Studies on the Internet of Things (Nicolescu et al., 2018) and social media (Kapoor et al., 2018) demonstrate how integrating these technologies can drive significant economic benefits through enhanced data analytics and improved user engagement. Further, the review includes studies comprising analysis of people analytics' expanding role in human resource management (Giermindl et al., 2022), illustrating its potential to transform traditional HR functions into strategic activities that directly contribute to the bottom line. We have also incorporated the studies that examine the challenges and opportunities of conversational agents (Diederich et al., 2022) and innovative technologies like neuro-based decision support systems for employee recruitment (Zazon et al., 2023), which can significantly reduce hiring costs and increase precision in candidate selection. Additionally, our review covers studies on gig workers' perceptions of algorithmic control with a focus on privacy (Wiener et al., 2023), emphasizing economic implications on employee satisfaction and retention. The adoption of Identity-as-a-Service for identity and access management (Mikhaeil & James, 2023) and the impact of feature-based explanations in modern AI systems on user decision-making (Bauer et al., 2023) are also included, illustrating how AI can streamline operations and reduce costs related to security and user training. Our review also encompasses studies that discuss the rise of connected workplace surveillance (Mettler, 2023) and the unintended control and exploitation of digital trace data tools (Nyman et al., 2023), underscoring the economic implications of surveillance technologies in terms of both operational efficiency and potential risks to employee trust and corporate reputation.

As the IS field transitions to an era marked by big data-driven transformations, the ethical dimensions of AI in the IS domain have garnered significant attention in the literature. A foundational study by Wakunuma and Stahl (2014) underscores the importance of foresight and future research in addressing these ethical issues, particularly concerning the intersection of technology and human actors within socio-technical systems. Our systematic review includes studies that illuminate the ethical concerns that surface from various technology applications. For instance, integrating wearable devices in corporate wellness programs raises questions about how much surveillance an employer can exercise over an employee's personal health data (Yassaee et al., 2019). Similarly, implementing the General Data Protection Regulation (GDPR) has significant implications for start-up companies focused on AI innovation, spotlighting the tension between regulatory compliance and technological advancement (Martin, 2019a). The discussion extends to the severity of whaling cyberattacks and their ethical ramifications (Pienta et al., 2020), emphasizing the need for robust security measures that do not infringe on personal privacy. The literature also explores the delicate balance between leveraging analytics for business benefits and protecting individual privacy. Studies such as those by Alter (2020) critique the invasive potential of "smart" technologies, while Young et al. (2020) investigate the ethical implications of advanced IS programs on stakeholders' privacy.

Further research delves into technology-mediated control (Cram & Wiener, 2020), augmented intelligence (Jain et al., 2021), and algorithmic decision-making systems (Marabelli et al., 2021), each presenting complex ethical challenges in the workplace, such as the dilemma posed by non-explainable AI systems (Asatiani et al., 2021). Moreover, the synthesis examines the studies that emphasize the applications of deep reinforcement learning in enhancing cybersecurity measures (Sewak et al., 2021) while concurrently addressing the ethical considerations necessary in IS research (Mirbabaie et al., 2022). By incorporating

studies focused on the ethical management of human-AI interactions and the socio-materiality of workplaces (Heyder et al., 2023), the review list the studies that provide a comprehensive exploration of the diverse ethical perspectives essential for navigating the digital landscape responsibly.

Our systematic review has included a series of influential studies that also shed light on the social impacts of AI on employee privacy, providing a comprehensive understanding of the intersection between technology and human actors. One such study by Mitrokotsa et al. (2010) explicitly highlights the data security vulnerabilities associated with RFIDs, providing a foundational understanding that has guided the development of more efficient countermeasures to enhance RFID system security. This sets the stage for addressing broader social implications, such as the governance challenges in technology-mediated knowledge sharing, which present a comprehensive view of the evolving AI landscape. Our review also includes research by Okeke and Eiza (2022), which explores challenges preventing internal identity theft-related crimes in the UK retail sector. This study contributes to understanding the risk associated with identity loss due to technological advancements. Furthermore, examining phishing vulnerabilities among employees (Wright et al., 2023) and the implications of the EU's GDPR (Labadie & Legner, 2023) captures the evolving complexities of employee privacy in the digital age. Additional included studies such as those on cloud computing adoption challenges (Polyviou et al., 2023), the influence of paternalistic leadership on information security policy compliance (Zhu et al., 2023), and the application of AI governance in the energy sector (Papagiannidis et al., 2023) provide insights into contemporary challenges and opportunities. These studies underscore the social dynamics influenced by AI, revealing how technological governance can impact organizational behavior and employee interactions. Lastly, our synthesis covers the barriers to responsible AI implementation (Merhi, 2023), the transition from AI ethics to governance (Koniakou, 2023), and the distinguishing of AI ethics issues from conventional IS applications (Niederman & Baker, 2023). These topics offer a panoramic view of the evolving IS landscape, emphasizing the social ramifications of AI technologies in various sectors and their implications for employee privacy and organizational practices.

This comprehensive synthesis highlights the evolving themes of economic, ethical, and societal implications linked with AI-employee privacy concerns. It underscores the need to examine the benefit-costs for employees associated with the employment of AI in organizational settings in the ever-changing digital landscape, as discussed below.

4.2 Privacy Calculus and Advancing AI

This section explores the varying impacts of the advancing nature of AI technologies on employee privacy calculus, as detailed in Table 2. As organizations increasingly adopt AI-driven processes, understanding how each type of AI technology—descriptive, predictive, prescriptive, and autonomous—interacts with and influences employee data privacy calculus becomes critical. By delving into each technology's specific characteristics and effects, we aim to provide a nuanced understanding of how AI shapes employees' privacy calculus, balancing operational gains and privacy safeguards.

4.2.1 Privacy Calculus and Descriptive AI

Descriptive AI technology, utilized in organizational settings for employee surveillance and job evaluation, primarily functions by monitoring and analyzing workplace activities. This technology systematically collects data on employee actions, which is then processed to identify patterns and trends that aid in performance evaluation and operational decision-making (Wiener et al., 2023). Integrating descriptive AI in the workplace could benefit employees by enhancing fairness and efficiency in daily operations. This AI technology offers a clear, objective overview of their activities, which supports transparent and data-driven decision-making. Such an environment ensures that performance evaluations are based on quantifiable, unbiased data rather than subjective opinions, which can often be influenced by personal bias or incomplete information. This level of objectivity in assessing performance could help to ensure that all employees are evaluated fairly, promoting a sense of equity and trust within the team. Moreover, descriptive AI contributes to overall operational efficiency, streamlining workflows and identifying areas for improvement. This not only helps employees focus on their most impactful tasks but also reduces the unnecessary stress of manual tracking and self-reporting, allowing them to dedicate more energy towards creative and strategic functions.

Despite its advantages, deploying descriptive AI raises significant concerns, particularly regarding employee privacy. The extensive data collection required by such AI systems can lead to over-surveillance, potentially encroaching on personal spaces and diminishing trust within the workplace. For

instance, Microsoft's "workplace analytics" monitor the employees' basic job-related data such as time-spent on websites, email response rates, and speed of writing emails (Wujciak, 2019). With such technologies, employees may feel that their personal interactions are being intrusively monitored when AI systems continuously analyze their emails and communications for productivity assessments. This perception can erode trust and contribute to a stressful work environment (Cardon et al., 2023). Moreover, managers might develop unwarranted confidence in the system's outputs, possibly overlooking its limitations. An example is the reliance on AI-driven performance metrics, which may fail to consider the context of team dynamics and individual challenges, leading to misinterpretations and unfair evaluations of employee performance. Such scenarios underscore the need for critical oversight of privacy considerations in implementing descriptive AI technologies in the workplace.

4.2.2 Privacy Calculus and Predictive AI

Predictive AI, characterized by its capability to forecast future developments through historical or real-time data analysis, plays a crucial role in organizational decision-making. This technology utilizes sophisticated algorithms to predict outcomes and assign probabilities to future scenarios, enabling continuous monitoring and valuable insights supporting management decisions (Bauer & Gill, 2023). The integration of predictive AI in business processes offers substantial benefits. Firstly, predictive AI's ability to anticipate future trends and analyze potential scenarios empowers employees to be more proactive rather than reactive. This foresight allows them to prepare better for upcoming changes, which can reduce the stress and uncertainty often associated with rapidly changing workplace demands. Additionally, by leveraging predictive AI to optimize operations and tailor marketing strategies, employees can engage in more targeted and efficient work practices. This efficiency not only improves productivity but also enhances job satisfaction as employees can see the direct impact of their work in driving the company's success. Predictive AI's role in risk management also provides a safety net that helps ensure that employees are not caught off-guard by potential disruptions. This can lead to a more stable work environment where employees feel secure and supported in their roles. Furthermore, predictive AI allows employees to contribute more strategically to the organization. By providing insights and data-driven predictions, employees are equipped with the tools necessary to make informed decisions and offer valuable contributions to strategic discussions. This elevates their role within the organization and fosters a sense of accomplishment and career growth, as they can directly influence key business outcomes.

Despite its advantages, deploying predictive AI introduces several privacy challenges, primarily due to the complexity and obscurity of its underlying algorithms. As these algorithms become increasingly intricate, understanding and interpreting the basis of their predictions becomes more challenging (Martin, 2019b). For example, Amazon's tracking system monitors the movement of workers at the workplace to evaluate their efficiency (Lecher, 2019), this AI system could categorize these employees based on their productivity, which could further facilitate decision-making for human managers. Similarly, the Amazon wristbands can record the precise hand movement of the workers while they retrieve or steer the items at the requisite location within the warehouse (Yeginsu, 2018), thus generating insights into process efficiency. Though employers resort to various measures entailing second-generation AI to keep a tab on the continuous activities of employees through wearable sensors, cameras, and smartphones (Goyal, 2018) for facilitating decision-making through processed insights, such predictive AI systems have extreme potential to violate the privacy domain of the employees.

4.2.3 Privacy Calculus and Prescriptive AI

Prescriptive AI, characterized by algorithms that automatically generate decision recommendations using advanced statistics, scenarios, and machine learning techniques, introduces a transformative approach to organizational decision-making (Marabelli et al., 2021). This technology leverages complex models to provide data-driven recommendations, enhancing decision-making across various business contexts. Incorporating prescriptive AI within organizations offers benefits that are multifaceted and impactful. By automating the decision-making processes that typically require extensive data analysis, prescriptive AI significantly reduces the cognitive load on employees. This allows staff to allocate more time and energy towards creative and higher-level strategic tasks, rather than getting bogged down by the often tedious and time-consuming aspects of data crunching and scenario analysis. Furthermore, prescriptive AI's ability to analyze multiple scenarios and predict outcomes enables employees to work with a higher degree of confidence in the decisions they make or support. This is particularly crucial in dynamic environments where swift, accurate decisions can differentiate between success and failure. With prescriptive AI, employees can rely on data-driven recommendations, reducing uncertainty and enhancing

their capability to respond effectively to changing conditions. This boosts individual performance and enhances overall job satisfaction as employees feel more empowered and supported by reliable, intelligent systems.

However, the use of prescriptive AI comes with notable privacy challenges, primarily stemming from the complexity of its algorithms. These algorithms can be so intricate that they exceed the comprehension abilities of the employees and managers interacting with them. Without a clear understanding of the algorithm's rationale, these recommendations may be perceived as arbitrary or misguided, leading to resistance or incorrect implementation (Gal et al., 2020). For instance, as we extend on our example of Amazon that utilizes evolving AI artefacts in the workplace, the workers in the Amazon fulfillment centre who are unable to meet productivity quotas are automatically sent warnings or termination letters without any human interference through the recording and accounting of invasive details of employees, such as their “off-task” time and thus, placing tracking-and-firing power in the hands of AI systems (Tangermann, 2019). Such AI has the externalities of active ability to penetrate non-relevant aspects of employees, infiltrate private information, and even employ unethical methods for inquiry of employees (Stahl & Wright, 2018). Another example of such technological usage is from Walmart. In 2018, Walmart patented an AI system with “sound sensors”, which surreptitiously listen to subtle sounds such as an employee's greeting of guests, conversations of the guests in line, rustles of the bags, and beeps of scanners at the check-out line, to track the performance of employees and augmenting autonomous decision-making for their job appraisals (Saha, 2018). Hence, the impact of technology control on employee decision-making and the high risks of succumbing to private information could drastically alter the employee privacy calculus for such prescriptive AI systems in the organization.

4.2.4 Privacy Calculus and Autonomous AI

Autonomous AI, characterized by its ability to autonomously derive complex decisions, execute them, and communicate outcomes based on self-learning processes, including emotional learning, introduces a transformative yet challenging dimension to organizational operations (Mullins et al., 2022). This advanced technology manages and regulates activities with an extensive understanding of emotional nuances, enhancing the adaptability and responsiveness of organizational processes. The primary benefit of autonomous AI lies in its ability to automate complex decision-making processes, significantly enhancing workplace efficiency and adaptability. This automation frees employees from the monotony and potential errors associated with routine decision-making tasks and allows them more time to focus on more creative, strategic, and intellectually stimulating aspects of their roles. Moreover, the capacity of autonomous AI to adapt and respond in real-time to changing conditions can create a more dynamic and responsive work environment (McStay, 2020). This adaptability helps ensure that organizational processes remain efficient and effective, directly contributing to a more secure and prosperous work setting for employees.

However, deploying autonomous AI also presents significant challenges, primarily related to its opaque nature. The intricate algorithms and self-learning capabilities that enable autonomous AI to act without human intervention can make its decisions and actions difficult to trace and understand. This obscurity can lead to a lack of accountability, creating feelings of powerlessness among employees and challenges in managerial oversight. The difficulty in tracing decisions back to a rationale can foster information asymmetries, obscure organizational power structures, and complicate governance processes. Furthermore, there is often a notable level of resistance or aversion to algorithms among employees, who may distrust or fear the implications of such technology on their roles and privacy.

4.3. Alternatives to Mitigate the Privacy Concerns

To address the privacy concerns associated with AI, the existing IS literature suggests a multi-faceted approach that emphasizes transparency and managerial accountability to integrate specific mechanisms and technologies aimed at safeguarding privacy.

One such strategy involves designing mechanisms of information disclosure that communicate how data is used and highlight the benefits of such disclosure to increase user trust and compliance. Mikhaeil and James (2023) emphasize the importance of clearly articulating the advantages of information sharing to encourage more informed and favorable attitudes toward data use in AI systems. Additionally, the development of technologies such as explainable AI is critical to reducing the information asymmetry between users and algorithms (Bauer et al., 2023). This approach aims to make AI decisions more

transparent and understandable to users, thereby fostering trust and reducing apprehensions about AI processes.

Moreover, using technologies like RFID, as discussed by Mitrokotsa et al. (2010), can enhance the security of user data, providing robust protection against unauthorized access and misuse. Executing design principles that enhance information transparency is another vital step in addressing privacy concerns. Lyytinen and Grover (2017) outline the importance of implementing such principles to improve how information is presented and accessed, enabling better user understanding and management of privacy risks. Furthermore, planning alternatives that balance the privacy costs with the benefits derived from the information provider is essential. Nicolescu et al. (2018) suggests that carefully weighing the trade-offs between privacy and the advantages of data disclosure can lead to more equitable and acceptable data practices. This involves evaluating how the benefits of AI can be maximized for users (including employees) while minimizing the intrusion into their personal data.

Despite these proposed measures, it is evident that they may not be adequate to minimize the risks associated with the advancing adoption of AI in organizations and its implications on employee privacy. As AI technologies become more integrated into organizational processes and decision-making, the challenges of ensuring privacy, accountability, and ethical compliance become more complex and demanding. This necessitates ongoing research, updated regulatory frameworks, and continuous improvement in AI governance practices to ensure that the benefits of AI are leveraged responsibly while mitigating potential risks to employee privacy and organizational integrity.

5 Research Gaps and Future Research Areas

This section presents the research gaps in the existing literature and future research opportunities for scholars working in the domain of IS and AI from the systematic literature review.

5.1 Multiple AI Definitions and its Varied Classifications

The swift advancement of AI has created a significant challenge due to the lack of a consistent definition and classification system. As AI continues to develop, its conceptual boundaries become increasingly complex, complicating the task of distinguishing its various forms. This inconsistency in definitions and the multitude of AI types contribute to an ambiguous and dispersed understanding of the implications of AI and its diverse classifications. Academic discourse on AI reflects this uncertainty. For instance, Kaplan and Haenlein (2019) advocate for a four-category classification of AI, while other scholars propose a three-tiered approach, further adding to the complexity of comprehending AI's multifaceted nature. We have adopted the four types of advancing AI outlined by Giermindl et al. (2022) as this classification provides a relatively clear demonstration of the capabilities of AI to perform varied functions and has been recognized in recent work within the IS journal.

Through our systematic review, we suggest that the distinct characteristics of different AI types necessitate a meticulous examination of the contractual frameworks that organizations employ when adopting these technologies. The inconsistency in defining or classifying AI types requires a need for a unified definition to ensure a consistent understanding and to grasp its implications on employee behavior. Hence, to effectively address the evolving use of AI in the workplace, it is imperative for future AI and IS researchers to conduct comprehensive investigations into how different AI categories impact employee behavior.

The current lack of clear definitions and distinctions among AI categories complicates the governance of these technologies, which can profoundly influence how employees interact with AI and adapt to new workflows and decision-making processes. Such research is crucial for developing more sophisticated and effective strategies to manage the complex dynamics between AI technology and employees' perception toward it. By doing so, researchers can ensure that advancements in AI are implemented responsibly and ethically, fostering an environment where technological innovation supports organizational goals and employee well-being. This proactive approach will enhance understanding and guide the development of best practices for AI use across industries.

5.2 Complexity of AI-privacy Integration

Previous research has extensively highlighted both the positive and negative effects of generic AI on employee privacy, identifying its capacity to enhance operational efficiencies and its potential to infringe

on personal privacy (Dincelli & Yayla, 2022; Mettler, 2023; Vial, 2019). These studies have set a foundational understanding of AI's broad impacts within organizational contexts but have often left the deeper, more specific implications of advanced AI technologies less explored.

In response to this gap, our comprehensive review examined 55 studies focusing on the analytical maturity of AI technology and its specific implications for employee privacy. We observed a significant evolution in AI's capabilities, transitioning from basic, request-driven historical reporting to more sophisticated, predictive, and algorithmic applications that increasingly influence various aspects of organizational operations (Mettler, 2023; Bauer & Gill, 2023). This shift, illustrated in Table 1, highlights the complexities and developmental stages of AI technology, providing critical insights into how the maturation of AI affects privacy considerations.

However, as AI systems become more dynamic and their operational processes grow in complexity—often surpassing human cognitive capabilities—traditional privacy safeguards may prove inadequate (Marabelli et al., 2021; Yassaee et al., 2019). The advancement of AI technologies necessitates a reassessment of current data governance and contractual frameworks to ensure they are robust enough to protect employee privacy in this rapidly evolving landscape.

Therefore, future AI and IS researchers must focus on thoroughly investigating the specific impacts of advancing AI on employee privacy. This involves exploring how emerging AI functionalities, which include complex algorithmic processes and extensive data utilization, could undermine existing privacy protections (Liu et al., 2022). Researchers need to develop and suggest adaptable, innovative privacy solutions that are capable of coping with the increased sophistication of AI technologies. Such studies are crucial for enhancing our understanding of the nuanced relationship between AI advancement and employee privacy, and for developing strategic frameworks that align technological innovation with ethical standards and privacy protections in workplaces. This focus will contribute to the academic discourse and provide practical guidance for organizations aiming to implement AI responsibly.

5.3 Need for Distinct Privacy Calculus of Employees

This systematic review of IS literature underscores a notable gap in exploring employee privacy calculus within the context of advancing AI technologies in organizational settings. Although the benefits and costs to employees regarding data sharing are well-documented (Nicolescu et al., 2018), there remains a significant need to understand how various AI technologies, each with unique information processing and exchange capabilities, impact the psychological contracts of employees due to privacy breaches.

Descriptive AI primarily functions in organizational settings to monitor and report on employee activities. Highlighted in the works of Wiener et al. (2023), it provides managers with a clear view of workforce dynamics, enhancing transparency and efficiency. However, its continuous monitoring could be perceived as intrusive, fostering privacy invasion concerns and potentially decreasing employee satisfaction and morale due to the feeling of being constantly watched, which could also lead to legal concerns over privacy rights (Jain et al., 2021). Predictive AI uses historical data to forecast future outcomes, allowing organizations to plan effectively and anticipate future trends and behaviors. Bauer and Gill (2023) note that while this technology aids informed decision-making, the assumptions and biases within the algorithms can perpetuate existing prejudices, raising ethical concerns about fairness and discrimination. This can undermine employee trust in the fairness and integrity of AI-driven evaluations and decisions.

Prescriptive AI goes further by suggesting specific actions based on its analyses (Marabelli et al., 2021). While it enhances decision-making by providing optimized solutions, it also raises significant questions about employee autonomy. There is concern that such AI could diminish human decision-making roles, potentially leading employees to feel that their professional judgment is being undermined or replaced by automated processes, thus impacting their psychological contract with the organization. Autonomous AI (Mullins et al., 2022), operates with a high degree of independence and deeply integrates into personal and professional aspects of employees' lives. While it can significantly enhance efficiency and adaptability, its capacity to make decisions autonomously can be seen as highly intrusive, raising substantial privacy and trust concerns among employees. The fear that AI might make crucial decisions without human oversight or ethical consideration can lead to resistance from the workforce.

In essence, each AI technology presents distinct benefits and challenges to organizational settings, particularly regarding employee privacy. These dynamics necessitate careful management to ensure that AI deployments align with ethical standards and respect employee privacy and autonomy. This understanding underscores the need for a more elaborate framework linking the progression of AI

technologies with the concept of employee privacy calculus. As AI continues to evolve, organizations face the challenge of addressing unforeseen privacy consequences, requiring ongoing vigilance and adaptive policy measures. This discourse on employee privacy calculus in the context of AI is still developing (Mikhaeil & James, 2023).

Table 1. AI Implication on Privacy Calculus of Employees

AI maturity level	Descriptive AI	Predictive AI	Prescriptive AI	Autonomous AI
Characteristics	AI algorithms examine past events and their influence on the present (Wiener et al., 2023)	AI algorithms predict future developments by analyzing past or real-time data and assigning probabilities to different scenarios (Bauer & Gill, 2023)	AI algorithms automatically generate decision recommendations using advanced statistics, scenarios, and machine learning techniques (Marabelli et al., 2021)	AI algorithms autonomously derive complex decisions, execute them, and communicate them based on self-learning processes, including emotions learning (Mullins et al., 2022)
Privacy Calculus	From a privacy calculus perspective, sharing personal data with the organization brings benefits like improved individual performance and accurate appraisals through monitoring. However, these advantages must be weighed against costs, including information loss, extended surveillance, and challenges in understanding advanced AI data processing. A thorough assessment is crucial to avoid legal and ethical issues. Scholars highlight factors disrupting privacy calculus, such as underestimating disclosure consequences, difficulty foreseeing outcomes, and evolving technology impacts on information sharing. (Mikhaeil & James, 2023; Markus, 2017), Laufer & Wolfe, 1977).			
Benefits	Precise monitoring and performance evaluation (Marabelli & Newell, 2023; Newell & Marabelli, 2015) Increased operational efficiencies and enhanced control of behaviour (Drydakis, 2022; Nyman et al., 2023) Opportunity for inclusive systems and societal improvements (Marabelli & Newell, 2023)			
Costs	Primarily includes; basic monitoring tools applied for employee surveillance and job performance evaluation Result: Employees may wrongly believe that digital data precisely depicts reality, fostering unwarranted confidence. Deciphering decision rationales via analytics demands statistical expertise. Managers are accountable for analytics-backed decisions in people-related matters, but employees can request rationale disclosure (Jain et al., 2021).	Primarily includes continuous monitoring, drawing insights and assisted management decision-making Result: The algorithms and justifications behind these decisions are predominantly obscure and progressively challenging to comprehend. Managers remain responsible for data-driven and technologically derived decisions, even though they may struggle to explain and justify them in a logically understandable manner (Alter, 2020; Marabelli et al., 2021)	Primarily includes behavioural analysis, creative task execution, tracking activities on and augmented decision-making Result: The complexity of algorithms can exceed the comprehension of both employees affected by their application and the managers who implement them. Assigning accountability for decision-making and actions at a specific human level becomes challenging, potentially resulting in decisions being viewed as arbitrary and irrational (Gal et al., 2020)	Primarily includes extensive regulating of activities using comprehensive emotions accounting Result: Opaque decisions create accountability challenges for employees, the organization, and analytics providers. This fosters a sense of powerlessness, hindering oversight and potentially obscuring power structures, leading to information asymmetries. High level of algorithm aversion in this context among the employees (Gal et al., 2020)
Alternatives to mitigate the potential risks of using AI	Designing mechanisms of information disclosure by suggesting the benefits of information disclosure (Mikhaeil & James, 2023) Development of technologies, such as explainable AI to reduce the information asymmetry between user and algorithm (Bauer et al., 2023). Also, usage of technologies, such as RFID to protect the user data (Mitrokotsa et al., 2010) Executing the design principles to enhance information transparency and related coping mechanisms (Lyytinen & Grover, 2017) Planning the alternatives of privacy cost with the benefits derived for the information provider (Nicolescu et al., 2018)			

Addressing this gap requires a multidisciplinary approach that integrates insights from IS, psychology, and organizational behavior. Future research should explore the specifics of AI technologies and their evolving impact on the employee-organization relationship, aiming to develop comprehensive, ethical, and privacy-conscious frameworks for AI integration in workplaces. This approach will enrich academic understanding and guide organizational practices and policy development in the rapidly advancing AI landscape.

5.4 AI-ethics Perspective

In the nascent field of AI research pertaining to employee privacy, our findings signal the need for more profound investigation. Future research should explore AI's effects on the various dimensions of employees' professional lives, encompassing self-identity, career development, stress, and engagement. A comprehensive approach transcending privacy concerns is required to reveal the full implications of integrating advanced AI in the workplace. Furthermore, the rise of empathetic intelligence in AI beckons a novel research domain (Huang & Rust, 2018). As AI systems grow more adept at understanding human emotions, it becomes imperative to understand how this emotional acuity affects privacy dynamics, aiming to proactively address the ethical quandaries posed by such emotionally aware AI technologies (Benbya et al., 2021).

The shift towards AI systems with heightened emotional intelligence amplifies the stakes for organizational privacy, potentially transforming human roles within corporate procedures. This evolution necessitates an ethical inquiry into the influence of super-intelligent AI on organizational privacy practices. Crafting ethical guidelines and policies for the deployment of advanced AI is essential, ensuring responsible application within business contexts. Consequently, examining AI's impact on employee privacy becomes a complex endeavor, extending beyond prevailing discussions to a wider examination of its extensive effects on individual and organizational dynamics, underscoring the imperative for holistic research that informs both theoretical frameworks and practical applications.

5.5 Lack of Empirical Research in the Space of Advancing AI-employee Privacy

In the realm of IS research, there exists a notable gap in empirical studies specifically addressing AI's impact on employee privacy, in contrast to the broader focus on consumer privacy. This oversight limits the comprehensive understanding of how AI influences privacy dynamics within the workforce, despite its growing presence and transformative role in modern organizations (Cheng et al., 2022; Hui et al., 2007). Given AI's rapid integration into organizational systems and decision-making processes, it is critical that future research focuses on examining its effects on employee privacy, an aspect that remains underexplored in the existing IS literature (Diederich et al., 2022).

Furthermore, the field of Industrial and Organizational Psychology recognizes the complexity of these privacy issues within the context of advancing AI (Bostrom, 2020), yet this nuanced perspective is often insufficiently mirrored in IS research. A detailed, multidisciplinary investigation is necessary to understand how AI's rapid proliferation within organizational structures affects employees' experiences of privacy.

The evolving regulatory landscape surrounding AI usage introduces additional complexity (Labadie & Legner, 2023). As governments and regulatory bodies ramp up their oversight, there is an increased urgency for comprehensive, in-depth research within the IS domain. This research is essential for advancing academic discourse and guiding the development of informed organizational policies that balance technological advancement with privacy protections.

Moreover, with the emergence of AI systems equipped with empathetic intelligence, a new field of inquiry is beckoning (Huang & Rust, 2018). As these systems become more proficient at understanding human emotions, exploring how their emotional acuity impacts privacy dynamics is crucial. This exploration must aim to proactively address the ethical dilemmas posed by such emotionally aware AI technologies (Benbya et al., 2021).

Integrating AI systems with enhanced emotional intelligence raises significant concerns for organizational privacy, potentially altering human roles and interactions within corporate processes. This transformation underscores the need for an ethical examination of how super-intelligent AI influences organizational privacy practices. The development of ethical guidelines and policies for deploying such advanced AI technologies is paramount to ensure their responsible application within business contexts.

Thus, examining AI's impact on employee privacy evolves into a complex endeavor that extends beyond current discussions to a broader examination of its extensive effects on both individual and organizational

dynamics. This necessitates holistic research that informs and enriches both theoretical frameworks and practical applications, ensuring that the deployment of AI technologies within organizations is both ethically sound and beneficial.

6 Implications of the Study

Our research underscores the emerging field of AI and employee privacy, elucidating various applications. This integrative review enhances the theoretical comprehension of the AI-employee privacy nexus within IS. By adopting a comprehensive perspective on AI's impact on employee privacy, our study transcends disciplinary boundaries and synthesizes findings from diverse fields. This inclusive approach allows us to present contemporary and holistic insights into the intricate implications of advancing AI technologies on employee privacy in organizational contexts. The subsequent section explores the theoretical implications, offering valuable insights for IS researchers, practitioners, and policymakers.

6.1 Contribution to Information Systems Research

This manuscript makes four theoretical contributions to the field of IS by addressing crucial aspects of AI integration and employee privacy within organizational contexts. First, we introduce a contemporary framework that systematically organizes existing knowledge on AI and employee privacy. This framework integrates multidisciplinary perspectives, including ethical considerations, decision-making dilemmas, and compliance with legal standards, offering a comprehensive analysis that surpasses previous reviews (e.g., Enholm et al., 2022; Heyder et al., 2023).

Second, our integrative systematic review highlights AI's dynamic and evolving nature, addressing the critical need for a domain-specific discussion beyond the generic viewpoints prevalent in existing literature (Mettler, 2023; Vial, 2019). Our work rigorously dissects the changing paradigms of AI, particularly emphasizing its implications for workplace privacy, an area that has received limited focus thus far. Through our comprehensive framework, we identify and articulate crucial gaps in both empirical and theoretical domains of AI research, which has traditionally underexplored the nuanced impact of AI on employee privacy. We present an elaborate synthesis of the current research, methodically mapping the intellectual landscape to guide future scholarly endeavors. This mapping not only elucidates the areas lacking robust research but also proposes new avenues for inquiry, adapting continuously to the rapid advancements in AI technologies. By fostering a deeper understanding of the evolving implications of AI-driven surveillance on employee privacy, our review is a foundational resource that encourages further exploration into these less charted waters. The targeted research questions we propose are specifically designed to probe into these dynamic aspects, setting the stage for future research that can build upon our findings to advance the discourse in the IS community significantly.

Third, the current literature predominantly consists of systematic reviews with a narrow focus on specific AI applications within organizational settings (e.g., Enholm et al., 2022; Heyder et al., 2023), primary surveys and interviews of concerned stakeholders (e.g., Mikhaeil & James, 2023; Fox & James, 2021; Mettler, 2023), and perspective pieces on AI applications or detection techniques (e.g., Marabelli & Newell, 2023; Sewak et al., 2023). While valuable, these studies often lack a holistic view and do not construct a robust theoretical framework that adequately addresses the broad implications of AI on employee privacy. Our review uniquely addresses this gap by systematically compiling and analyzing literature that spans multiple dimensions of AI applications and their privacy implications, providing a broader perspective that has been largely absent in current research. Furthermore, most existing studies lack a robust theoretical framework integrating advancing AI technologies with the complex dynamics of employee privacy (Benbya et al., 2021; Jain et al., 2021). Our work contributes significantly to this area by developing an overarching framework that synthesizes existing findings and guides future research on the intersection of AI and privacy (refer to Table 2).

Table 2. Comparison with some of the Extant Reviews

Study	Focus Area	Key Findings	Our Contribution
Enholm et al. (2022); Heyder et al., 2023	Specific AI applications in organizations and Employee perspectives on AI	Highlighted narrow impacts of AI on business processes and discussed general employee concerns	Broad examination of AI's multifaceted impact on privacy and detailed exploration of privacy calculus in AI context

Mikhaeil & James (2023); Fox & James, (2021); Mettler, (2023); Papagiannidis et al., (2023); Wiener et al., (2023)	Stakeholder surveys and interviews	Focused on concerns regarding specific AI tools	Integrated framework for AI privacy calculus
Marabelli & Newell (2023); Sewak et al., (2023)	Perspective pieces on AI detection techniques	Provided insights into specific AI applications	Comprehensive analysis across multiple AI dimensions

Last, our review highlights a significant gap in the exploration of employee privacy calculus in the context of advancing AI technologies within organizational settings. Expanding on the theoretical implications of privacy calculus (Mikhaeil & James, 2023), our study explores how shifts in privacy calculus occur amidst the widespread integration of AI technologies. Privacy calculus, traditionally understanding the trade-off between the benefits and the perceived risks of data sharing among employees, is critical as AI becomes pervasive in organizational settings. Our work challenges IS researchers to address these evolving considerations through innovative solutions that uphold ethical standards while fostering technological progress. We assert that as AI technologies advance, they reshape the landscape of employee privacy considerations by altering the balance between benefits and risks associated with data sharing. The introduction of various AI technologies—from descriptive to autonomous—raises complex questions about surveillance, data bias, decision-making autonomy, and the transparency of AI processes. These factors compel a re-evaluation of the privacy calculus framework within contemporary workplaces.

Our paper synthesizes existing research on AI and employee privacy to offer a multi-dimensional view that integrates diverse scholarly contributions. We emphasize the evolving nature of AI technologies and their complex impacts on privacy calculus, urging a balanced exploration of these advancements against ethical standards to protect employee privacy in increasingly digital environments. This integration enriches the theoretical corpus within the information systems field (Robert et al., 2020; Teebken & Hess, 2021), laying a robust foundation for future research to navigate both theoretical nuances and practical implications of AI in workplace privacy.

6.2 Implications for Practitioners and Managers

In IS research, the focus on privacy management often revolves around broad strategies like policy enforcement and trust-based disclosure (Bauer et al., 2023; Heyder et al., 2023). These approaches, however, may not fully capture the nuances of employee privacy calculus, particularly as AI's capabilities continue to evolve. As AI technologies become more embedded in everyday business operations, traditional privacy management methods increasingly fall short, potentially leading to ethical breaches and damage to organizational reputation. It is essential to develop comprehensive strategies that leverage AI's benefits and prioritize preserving employee privacy and strengthening organizational trust. To address these challenges, we propose several practical, actionable strategies for practitioners.

First, we advocate for leveraging technologies like RFID (Mitrokotsa et al., 2010) to add an extra layer of protection to user data. Such technologies enforce privacy safeguards automatically and that can include mechanisms like AI-driven pseudonymization of personal data before analysis. This approach minimizes privacy risks while allowing organizations to glean valuable insights from the data they collect. Integrating RFID helps ensure that privacy protection is built into the fabric of technological operations, offering a proactive approach to privacy management that is both effective and scalable.

Second, it is crucial for organizations to establish transparent communication about AI data practices (Mikhaeil & James, 2023). This involves explicitly outlining what data is collected, how it is utilized, and the measures implemented to protect it. Transparency builds trust and empowers employees by clarifying how their data is handled. For example, integrating explainable AI can bridge the information gap between users and algorithms (Bauer & Gill, 2023). Establishing open channels for employees to express concerns or request information about data usage further enhances this trust, making transparency a cornerstone of ethical AI deployment.

Third, a participatory design approach to AI system development is highly recommended. By involving employees in the creation and implementation of AI systems, organizations can address privacy concerns more effectively and ensure that the systems align with user expectations and needs. This approach helps fine-tune the technology to suit the specific privacy concerns of employees and fosters a sense of

ownership and acceptance among the workforce, thereby enhancing the overall effectiveness of AI solutions.

Fourth, continuous education and training on AI capabilities are required to resolve privacy issues. As AI technology evolves rapidly, keeping HR professionals and employees informed about the latest developments and potential privacy implications is crucial. Regular training programs can help demystify AI technologies, making it easier for employees to understand how AI works and its privacy implications, thus promoting a more informed and conscientious use of technology in the workplace. Alongside designing a strategic plan for incentives to reduce privacy costs, considering the benefits for information providers (Nicolescu et al., 2018) forms an integral part of the comprehensive approach to countering the negative implications of evolving AI on employee privacy.

Finally, implementing ethical AI frameworks that include strong privacy considerations is essential. These frameworks should guide the development and deployment of AI technologies, ensuring that ethical concerns are considered alongside technical and business objectives. An ethical AI framework helps balance the benefits of AI with the need to protect employee privacy, thus supporting sustainable and responsible use of AI in organizational settings. Through these measures, organizations can navigate the evolving AI landscape while safeguarding the privacy rights of their employees.

6.3 Implications for Policy Makers

Our study offers several key implications for policymakers navigating the complex interplay of AI and employee privacy. First, our research underscores the necessity for policymakers to comprehend and address the ethical considerations and potential risks associated with the pervasive integration of AI in workplace settings. As AI technologies continue to evolve, there is a pressing need for flexible and sensitive regulations to the specific contexts in which AI is employed. This approach should aim to move beyond rigid, one-size-fits-all solutions to embrace adaptive regulatory frameworks that can respond dynamically to the changing nature of AI technologies and their applications in various sectors. This ensures that regulations remain effective and relevant, safeguarding employee privacy without hampering the integration of new technologies.

Second, the study highlights several positive applications of AI that can enhance productivity and decision-making in organizational contexts. However, it also calls for balanced regulations that protect employee privacy while still fostering the beneficial uses of AI. Policymakers are encouraged to formulate regulations that prevent privacy invasions and support technological innovation and its positive contributions to the workplace. An example of such balanced regulation is the 2023 facial recognition technology law in Maryland, which mandates employer transparency and obtains consent before using advanced biometric tools during recruitment processes (Glasser & Forman, 2020; Gaines, 2023). This kind of legislation exemplifies protecting individual rights while not stifling technological advancement.

Next, as AI technologies rapidly advance, particularly in areas like detection algorithms, it becomes crucial for policies to keep pace and anticipate future developments. Policymakers should foster an environment that incentivizes the research and development of new AI technologies that come with robust privacy protections. Furthermore, collaboration with technology platforms to establish standards and guidelines for AI governance is essential. By doing so, policymakers can help create a comprehensive regulatory framework that supports responsible AI usage, effectively addresses emerging privacy concerns, and ensures that technological advancements contribute positively to society.

6.4 Implications for Employees

Our research highlights three critical implications for employees in the context of AI integration in the workplace. First, employees should become well-informed about their privacy rights and organizational AI policies. Understanding what data is collected, how it is used, and the measures to protect their privacy empowers employees to make informed decisions and advocate for their privacy. By familiarizing themselves with these policies, employees can better question and challenge any overreach or misuse of AI technologies (Mikhaeil & James, 2023).

Second, leveraging available privacy protection tools and settings provided by organizations is crucial. These tools can include options to opt out of specific data collection practices, adjust privacy settings on workplace devices, and use encryption for sensitive communications. Proactively managing these settings helps employees safeguard their personal information and maintain greater control over their privacy (Lyytinen & Grover, 2017).

Last, employees should actively participate in discussions about AI implementation within their organizations and advocate for the development and use of explainable AI technologies. Explainable AI reduces the information asymmetry between employees and AI systems by providing clear, understandable explanations for AI decisions, thus fostering trust and transparency (Bauer et al., 2023). Moreover, understanding the concept of privacy calculus for different AI technologies—such as descriptive AI, predictive AI, prescriptive AI, and autonomous AI—enables employees to evaluate the trade-offs between the benefits of AI integration and the potential privacy risks. This knowledge helps employees engage in informed dialogues with management and contribute to developing balanced and ethical AI practices within their organizations (Nicolescu et al., 2018). Also, employees are encouraged to participate in training sessions to understand AI technologies better (Cheng et al., 2022). Such involvement ensures that AI systems are designed and implemented with employee concerns in mind, fostering a more inclusive and transparent work environment.

By adopting these strategies, employees can play an active role in managing their privacy and ensuring that AI systems are implemented in ways that respect their rights while enhancing organizational efficiency. This collaborative approach between employees and management can lead to a balanced integration of AI, maximizing its benefits while minimizing privacy risks.

7 Limitations

While providing valuable insights, our research on AI and employee privacy is subject to several limitations. A primary limitation is our reliance on secondary data sourced mainly from academic studies in the IS literature. This methodological approach inherently narrows the scope of our analysis. Although we have included primarily IS literature to enrich our dataset, the diversity of sources remains limited. This constriction may overlook some nuanced interpretations and emerging concepts in the fast-evolving field of AI. Additionally, our study's framework is based on a set of predefined keywords searched across prominent databases, which may not capture all relevant studies due to the inconsistent nature of AI terminologies and the interdisciplinary impacts of AI on employee privacy. As a result, some pertinent studies might not have been included due to these search constraints or access limitations.

Further, this study's framework and data sources, while laying a solid foundation for understanding the broad impacts of AI on employee privacy, do not delve into the complexities introduced by individual differences in privacy perception. Our approach, therefore, might not fully encapsulate the personalized and context-specific nuances that influence privacy attitudes and behaviors in the face of AI integration in organizational settings. Our current study's scope does not extend to dissecting these individual variances comprehensively. We acknowledge this limitation, as the individual difference factor in privacy expectations could provide deeper insights into how employees perceive and react to AI-driven privacy in the workplace.

8 Conclusion

Our study offers a comprehensive integrative review of the literature at the juncture of AI and employee privacy. Recognized as crucial in the academic discourse (Torraco, 2005; Webster & Watson, 2002), this integrative review synthesizes existing research to form new insights and conceptual frameworks. Our paper stands out as one of the initial exhaustive reviews in this area, extending beyond previous works that focused on narrower aspects or specific domains.

In conducting this review, we have critically assessed the current literature, highlighting the essential facets of the AI and employee privacy dialogue that require further exploration. The framework proposed in our paper is designed to guide and structure future research in this field. We aspire for our review to act as a catalyst, encouraging interdisciplinary collaboration to explore the complex effects of AI on employee privacy. This collaborative exploration is vital for deepening our collective understanding, navigating the challenges, and capitalizing on the opportunities presented by this significant technological evolution.

References

Alter, S. (2020). Making sense of smartness in the context of smart devices and smart systems. *Information Systems Frontiers, 22*(2), *381-393*.

Asatiani, A., Malo, P., Nagbøl, P. R., Penttinen, E., Rinta-Kahila, T., & Salovaara, A. (2021). Sociotechnical envelopment of artificial intelligence: An approach to organizational deployment of inscrutable artificial intelligence systems. *Journal of the Association for Information Systems*, *22*(2), 325-252.

Ball, K., Daniel, E. M., & Stride, C. (2012). Dimensions of employee privacy: An empirical study. *Information Technology & People*, *25*(4), 376-394.

Bauer, K., & Gill, A. (2023). Mirror, mirror on the wall: Algorithmic assessments, transparency, and self-fulfilling prophecies. *Information Systems Research*, *INFORMS*, *35*(1), 226-248.

Bauer, K., Von Zahn, M., & Hinz, O. (2023). Expl(ai)ned: The impact of explainable artificial intelligence on users' information processing. *Information Systems Research*, *34*(4), iii-ix.

Bélanger, F., & James, T. L. (2020). A theory of multilevel information privacy management for the digital era. *Information Systems Research*, *31*(2), 510-536.

Benbya, H., Pachidi, S., & Jarvenpaa, S. (2021). Special issue editorial: Artificial intelligence in organizations: Implications for information systems research. *Journal of the Association for Information Systems*, *22*(2), 10.

Bhave, D. P., Teo, L. H., & Dalal, R. S. (2020). Privacy at work: A review and a research agenda for a contested terrain. *Journal of Management*, *46*(1), 127–164.

Bostrom, N. (2020). Ethical issues in advanced artificial intelligence. In *Machine ethics and robot ethics* (pp. 69-75). Routledge.

Brynjolfsson, E., & Mcafee, A. (2017). *The business of artificial intelligence*. Harvard Business Review. https://hbr.org/2017/07/the-business-of-artificial-intelligence

Cascio, W. F., & Montealegre, R. (2016). How technology is changing work and organizations. *Annual Review of Organizational Psychology and Organizational Behavior*, *3*, 349-375.

Cardon, P. W., Ma, H., & Fleischmann, C. (2023). Recorded business meetings and AI algorithmic tools: Negotiating privacy concerns, psychological safety, and control. *International Journal of Business Communication*, *60*(4), 1095–1122.

Cheng, X., Su, L., Luo, X. (Robert), Benitez, J., & Cai, S. (2022). The good, the bad, and the ugly: Impact of analytics and artificial intelligence-enabled personal information collection on privacy and participation in ridesharing. *European Journal of Information Systems*, *31*(3), 339–363.

Cram, W. A., & Wiener, M. (2020). Technology-mediated control: Case examples and research directions for the future of organizational control. *Communications of the Association for Information Systems*, *46*(1), 4.

Culnan, M. J. (1993). "How did they get my name?": An exploratory investigation of consumer attitudes toward secondary information use. *MIS Quarterly*, *17*(3), 341–363.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, *10*(1), 104-115.

Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues*, *59*(2), 323-342.

Diederich, S., Brendel, A. B., Morana, S., & Kolbe, L. (2022). On the design of and interaction with conversational agents: An organizing and assessing review of human-computer interaction research. *Journal of the Association for Information Systems*, *23*(1), 96-138.

Dincelli, E., & Yayla, A. (2022). Immersive virtual reality in the age of the Metaverse: A hybrid-narrative review based on the technology affordance perspective. *The Journal of Strategic Information Systems*, *31*(2), 101717.

Drydakis, N. (2022). Artificial Intelligence and reduced SMEs' business risks. A dynamic capabilities analysis during the COVID-19 pandemic. *Information Systems Frontiers*, *24*(4), 1223-1247.

Enholm, I. M., Papagiannidis, E., Mikalef, P., & Krogstie, J. (2022). Artificial Intelligence and business value: A literature review. *Information Systems Frontiers*, *24*(5), 1709–1734.

Gaines, D. E. (2023, July 18). *As employers expand artificial intelligence in hiring, Maryland is one of few states that have rules*. Maryland Matters. https://www.marylandmatters.org/2023/07/18/as-employers-expand-artificial-intelligence-in-hiring-maryland-is-one-of-few-states-that-have-rules/

Gal, U., Jensen, T. B., & Stein, M.-K. (2020). Breaking the vicious cycle of algorithmic management: A virtue ethics approach to people analytics. *Information and Organization*, *30*(2), 100301.

Glasser, N. M., & Forman, A. S. (2020). Facial recognition tech in Maryland job interviews. https://natlawreview.com/article/new-maryland-law-requires-applicant-consent-prior-to-using-facial-recognition

Giermindl, L. M., Strich, F., Christ, O., Leicht-Deobald, U., & Redzepi, A. (2022). The dark sides of people analytics: Reviewing the perils for organisations and employees. *European Journal of Information Systems*, *31*(3), 410–435.

Goyal, M. (2018, May 7). *Artificial intelligence: Your employer could be snooping on you, in office and outside*. The Economic Times. https://economictimes.indiatimes.com/jobs/your-company-may-be-spying-on-you-heres- why/articleshow/64045564.cms?from=mdr

Günther, W. A., Rezazade Mehrizi, M. H., Huysman, M., & Feldberg, F. (2017). Debating big data: A literature review on realizing value from big data. *The Journal of Strategic Information Systems*, *26*(3), 191–209.

Faverio, M. & Tyson, A. (2023, November 21). *What the data says about Americans' views of artificial intelligence*. Pew Research Center. https://www.pewresearch.org/short-reads/2023/11/21/what-the-data-says-about-americans-views-of-artificial-intelligence/

Fox, G., & James, T. L. (2021). Toward an understanding of the antecedents to health information privacy concern: a mixed methods study. *Information Systems Frontiers*, *23*(6), 1537-1562.

Hamilton, R. H., & Sodeman, W. A. (2020). The questions we ask: Opportunities and challenges for using big data analytics to strategically manage human capital resources. *Business Horizons*, *63*(1), 85–95.

Hao, K. (2019, November 11). *The computing power needed to train AI is now rising seven times faster than ever before.* MIT Technology Review. *Retrieved from* https://www.technologyreview.com/2019/11/11/132004/the-computing-power-needed-to-train-ai-is-now-rising-seven-times-faster-than-ever-before/

Heyder, T., Passlack, N., & Posegga, O. (2023). Ethical management of human-AI interaction: Theory development review. *The Journal of Strategic Information Systems*, *32*(3), 101772.

Higgins. J. P. (2008). Cochrane handbook for systematic reviews of interventions version 5.0.1. In *The Cochrane collaboration*. Cochrane Handbook. http://www.cochrane-handbook.org.

Huang, M. H., & Rust, R. T. (2018). Artificial intelligence in service. *Journal of Service Research*, *21*(2), 155-172.

Hui, K. L., Teo, H. H., & Lee, S-Y. T. (2007). The value of privacy assurance: An exploratory field experiment. *MIS Quarterly*, *31*(1), 19-33.

Jain, H., Padmanabhan, B., Pavlou, P. A., & Raghu, T. S. (2021). Editorial for the special section on humans, algorithms, and augmented intelligence: The future of work, organizations, and society. *Information Systems Research*, *32*(3), 675–687.

Kaplan, A., & Haenlein, M. (2019). Rulers of the world, unite! The challenges and opportunities of artificial intelligence. *Business Horizons, 63*(1), 37-50

Kapoor, K. K., Tamilmani, K., Rana, N. P., Patil, P., Dwivedi, Y. K., & Nerur, S. (2018). Advances in social media research: Past, present and future. *Information Systems Frontiers*, *20*, 531-558.

Koniakou, V. (2023). From the "rush to ethics" to the "race for governance" in artificial intelligence. *Information Systems Frontiers*, *25*(1), 71–102.

Labadie, C., & Legner, C. (2023). Building data management capabilities to address data protection regulations: Learnings from EU-GDPR. *Journal of Information Technology*, *38*(1), 16–44.

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues*, *33*(3), 22–42.

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

Liu, B., Pavlou, P. A., & Cheng, X. (2022). Achieving a balance between privacy protection and data collection: A field experimental examination of a theory-driven information technology solution. *Information Systems Research*, *33*(1), 203–223.

Lyytinen, K., & Grover, V. (2017). Management misinformation systems: A time to revisit? *Journal of the Association for Information Systems*, *18*(3), 206–230.

Marabelli, M., & Newell, S. (2023). Responsibly strategizing with the metaverse: Business implications and DEI opportunities and challenges. *The Journal of Strategic Information Systems*, *32*(2), 101774.

Marabelli, M., Newell, S., & Handunge, V. (2021). The lifecycle of algorithmic decision-making systems: Organizational choices and ethical challenges. *The Journal of Strategic Information Systems*, *30*(3), 101683.

Markus, M. L. (2017). Datification, organizational strategy, and IS research: What's the score? *The Journal of Strategic Information Systems*, *26*(3), 233–241.

Martin, K. (2019a). *Designing ethical algorithms*. MIS Quarterly Executive. http://dx.doi.org/10.2139/ssrn.3056692

Martin, K. (2019b). Ethical implications and accountability of algorithms. *Journal of Business Ethics*, *160*(4), 835-850.

McStay, A. (2020). Emotional AI, soft biometrics and the surveillance of emotional life: An unusual consensus on privacy. *Big Data and Society*, *7*(1), 2053951720904386.

Merhi, M. I. (2023). An assessment of the barriers impacting responsible artificial intelligence. *Information Systems Frontiers*, *25*(3), 1147–1160.

Mettler, T. (2023). 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.

Mikhaeil, C.A, & James, T. L. (2023). Examining the case of French hesitancy toward IDaaS solutions: Technical and social contextual factors of the organizational IDaaS privacy calculus. *Information & Management*, *60*(4), 103779

Mirbabaie, M., Brendel, A., & Hofeditz, L. (2022). Ethics and AI in information systems research. *Communications of the Association for Information Systems*, *50*(1), 38.

Mitrokotsa, A., Rieback, M. R., & Tanenbaum, A. S. (2010). Classifying RFID attacks and defenses. *Information Systems Frontiers*, *12*(5), 491–505.

Mullins, J., Stewart, P., & Greitens, T. (2022). Facing forward: Policy for automated facial expression analysis. *Journal of the Association for Information Systems*, *23*(6), 1347–1353.

Newell, S., & Marabelli, M. (2015). Strategic opportunities (and challenges) of algorithmic decision-making: A call for action on the long-term societal effects of 'datification.' *The Journal of Strategic Information Systems*, *24*(1), 3–14.

Nicolescu, R., Huth, M., Radanliev, P., & De Roure, D. (2018). Mapping the values of IoT. *Journal of Information Technology*, *33*(4), 345–360.

Niederman, F., & Baker, E. W. (2023). Ethics and AI issues: old container with new wine? *Information Systems Frontiers*, *25*(1), 9–28.

Nyman, S., Bødker, M., & Blegind Jensen, T. (2023). Reforming work patterns or negotiating workloads? Exploring alternative pathways for digital productivity assistants through a problematization lens. *Journal of Information Technology*, *39*(3), 503-520.

Okeke, R. I., & Eiza, M. H. (2022). The application of role-based framework in preventing internal identity theft related crimes: A qualitative case study of UK retail companies. *Information Systems Frontiers, 25*(2), 451-472.

Okoli, C. (2015). A guide to conducting a standalone systematic literature review. *Communications of the Association for Information Systems*, *37*.

Papagiannidis, E., Enholm, I. M., Dremel, C., Mikalef, P., & Krogstie, J. (2023). Toward AI governance: Identifying best practices and potential barriers and outcomes. *Information Systems Frontiers*, *25*(1), 123–141.

Pienta, D., Thatcher, J. B., & Johnston, A. (2020). Protecting a whale in a sea of phish. *Journal of Information Technology*, *35*(3), 214–231.

Polyviou, A., Venters, W., & Pouloudi, N. (2023). Distant but close: Locational, relational and temporal proximity in cloud computing adoption. *Journal of Information Technology*, 02683962231186161.

Rainie, L., Funk, C., Anderson, M., & Tyson, A. (2022, March 17). *How Americans think about artificial intelligence.* Pew Research Center. https://www.pewresearch.org/internet/2022/03/17/how-americans-think-about-artificial-intelligence/

Robert, L. P., Pierce, C., Marquis, L., Kim, S., & Alahmad, R. (2020). Designing fair AI for managing employees in organizations: A review, critique, and design agenda. *Human-Computer Interaction*, *35*(5–6), 545–575.

Saha, P. (2018, July 13). *Walmart patents tech tool to monitor employee performance*. https://www.hrkatha.com/hr-tools/walmart-patents-tech-tool-to-monitor-employee-performance/

Schlagwein, D., & Willcocks, L. (2023). 'ChatGPT et al.': The ethics of using (generative) artificial intelligence in research and science. *Journal of Information Technology*, *38*(3), 232–238.

Scully-Russ, E., & Torraco, R. (2020). The changing nature and organization of work: An integrative review of the literature. *Human Resource Development Review*, *19*(1), 66–93.

Sewak, M., Sahay, S. K., & Rathore, H. (2021). Deep reinforcement learning for cybersecurity threat detection and protection: A review. In *International Conference On Secure Knowledge Management In Artificial Intelligence Era* (pp. 51-72). Springer International Publishing.

Sewak, M., Sahay, S. K., & Rathore, H. (2023). Deep reinforcement learning in the advanced cybersecurity threat detection and protection. *Information Systems Frontiers*, *25*(2), 589-611.

Simbeck, K. (2019). HR analytics and ethics. *IBM Journal of Research and Development*, *63*(4/5), 9-1.

Simms, M. (1994). Defining privacy in employee health screening cases: Ethical ramifications concerning the employee/employer relationship. *Journal of Business Ethics*, *13*(5), 315–325.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, *35*(4), 989–1015.

Stahl, B. C., & Wright, D. (2018). Ethics and privacy in AI and big data: Implementing responsible research and innovation. *IEEE Security and Privacy*, *16*(3).

Syam, N., & Sharma, A. (2018). Waiting for a sales renaissance in the fourth industrial revolution: Machine learning and artificial intelligence in sales research and practice. *Industrial Marketing Management*, *69*, 135-146.

Tangermann, V. (2019). *Amazon used an AI to automatically fire low-productivity workers*. https://futurism.com/amazon-ai-fire-workers

Teebken, M., & Hess, T. (2021). Privacy in a digitized workplace: Towards an understanding of employee privacy concerns. In *Proceedings of the 54th Hawaii International Conference on System Sciences*.

Templier, M., & Paré, G. (2015). A framework for guiding and evaluating literature reviews. *Communications of the Association for Information Systems*, *37*(1), 6.

Torraco, R. J. (2005). Writing integrative literature reviews: Guidelines and examples. *Human Resource Development Review*, *4*(3), 356–367.

Torraco, R. J. (2016). Writing integrative reviews of the literature: Methods and purposes. *International Journal of Adult Vocational Education and Technology*, *7*(3), 62–70.

Vial, G. (2019). Understanding digital transformation: A review and a research agenda. *The Journal of Strategic Information Systems*, *28*(2), 118–144.

Wakunuma, K. J., & Stahl, B. C. (2014). Tomorrow's ethics and today's response: An investigation into the ways information systems professionals perceive and address emerging ethical issues. *Information Systems Frontiers*, *16*(3), 383–397.

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly*, *26*(2), xiii–xxiii.

Wiener, M., Cram, W. A., & Benlian, A. (2023). Algorithmic control and gig workers: A legitimacy perspective of uber drivers. *European Journal of Information Systems*, *32*(3), 485–507.

World Economic Forum. (2016). *The future of jobs employment, skills and workforce strategy for the fourth industrial revolution*. Global Challenge Insight Report. https://www.voced.edu.au/content/ngv:71706

Wujciak, M. (2019, October 18). *4 companies using machine learning to keep a close eye on employees*. CCW Digital. https://www.customercontactweekdigital.com/tools-technologies/articles/4-companies-u sing-machine-learning-to-keep-a-close-eye-on-employees

Wright, R., Johnson, S., & Kitchens, B. (2023). Phishing susceptibility in context: A multilevel information processing perspective on deception detection. *MIS Quarterly*, *47*(2), 803–832.

Yeginsu, C. (2018, February 1). *If workers slack off, the wristband will know. (And Amazon has a patent for it.)*. The New York Times. https://www.nytimes.com/2018/02/01/technology/amazon-wristband-tracking-privacy.html

Yassaee, M., Mettler, T., & Winter, R. (2019). Principles for the design of digital occupational health systems. *Information and Organization*, *29*(2), 77–90.

Young, J., Biros, D., Schuetzler, R., Smith, T., Stephens, P., Syler, R., & Zheng, S. (2020). When programs collide: A panel report on the competing interests of analytics and security. *Communications of the Association for Information Systems*, *46*(1).

Zazon, D., Fink, L., Gordon, S., & Nissim, N. (2023). Can NeuroIS improve executive employee recruitment? Classifying levels of executive functions using resting state EEG and data science methods. *Decision Support Systems*, *168*, 113930.

Zhang, A., Wang, C., Karahanna, E., & Xu, Y. (2022). Peer privacy concerns: Conceptualization and measurement. *MIS Quarterly*, *46*, 491–530.

Zhu, J., Feng, G., Liang, H., & Tsui, K. L. (2023). How do paternalistic leaders motivate employees' information security compliance? Building a climate and applying sanctions. *Journal of the Association for Information Systems*, *24*(3), 782-817.

Züger, M., Corley, C., Meyer, A. N., Li, B., Fritz, T., Shepherd, D., Augustine, V., Francis, P., Kraft, N., & Snipes, W. (2017). Reducing interruptions at work: A large-scale field study of FlowLight. In *Conference on Human Factors in Computing Systems - Proceedings*.

About the Authors

Prof. Kaur is an Assistant Professor at SP Jain Institute of Management and Research, specializing in human resource management and entrepreneurship. Her research explores leadership behavior and strategic organizational management, with both conceptual and empirical papers published in reputed journals. Her work has been presented at prestigious international and national conferences, such as the Academy of Management, Babson, the European Group of Organizations, and the Indian Academy of Management, where she has also won multiple best paper awards. Before earning her PhD from IIM-A in 2018, Prof. Kaur gained industry experience with McKinsey & Co, Deloitte USI, and ATOS Global and also ventured into entrepreneurship. Armed with degrees from the Delhi School of Economics and Shri Ram College of Commerce, she blends academic rigor with practical experience. Her research focuses on the intersection of technology, people management, and entrepreneurship, aimed at fostering sustainable business growth.

Prof. Sudhanshu Maheshwari is an Assistant Professor at SP Jain Institute of Management and Research, specializing in Human Resource Management and Organizational Behavior. He holds a Bachelor's in Electrical Engineering and a Master's in Economics from BITS Pilani, along with a Ph.D. from IIM Ahmedabad. His research focuses on the integration of technology with HRM and managerial and organizational cognition. Prof. Maheshwari's work has been accepted at prestigious management conferences such as the Academy of Management, the European Academy of Management, and the European Group of Organisational Studies. Additionally, he serves as a reviewer for peer-reviewed journals. His professional career includes roles as an Assistant Manager and Consultant, where he gained expertise in people management and strategic operations. His expertise lies in strategy, leadership, and human resource management.

Indranil Bose is Distinguished Professor of Information Systems at NEOMA Business School. He holds a BTech from the Indian Institute of Technology, MS from the University of Iowa, and MS and PhD from Purdue University. His research interests are in business analytics, digital transformation, information security, and management of emerging technologies. His publications have appeared in MIS Quarterly, Journal of the MIS, Communications of the ACM, Communications of the AIS, Computers and Operations Research, Decision Support Systems, European Journal of Operational Research, IEEE Transactions on Engineering Management, Information & Management, International Journal of Production Economics, Journal of the American Society for Information Science and Technology, Technological Forecasting and Social Change, Tourism Management etc. He serves as Senior Editor of Decision Support Systems, Journal of Organizational Computing and Electronic Commerce, and Pacific Asia Journal of the AIS; as Associate Editor of Communications of the AIS; and as Editorial Board Member of Information Systems Research.

Dr Simarjeet Singh is an Assistant Professor of Finance at the Great Lakes Institute of Management, Gurgaon, with expertise in portfolio management, fintech, financial econometrics, and behavioral finance. He is also a fellow and expert at the Digital Euro Association (a global think tank focusing on Central Bank Digital Currencies). He also served as an academic associate at the Indian School of Business (Mohali). His research explores the application of disruptive innovations in management, factor investing and portfolio management. Dr. Singh has published over 25 peer-reviewed articles in esteemed journals, including the Journal of Evolutionary Economics, Resource Policy, Management Review Quarterly, Online Information Review, Qualitative Research in Financial Markets, and International Social Science Journal and has reviewed over 30 research papers. He holds a Ph.D. in Finance from Punjabi University (Patiala), specializing in portfolio management, and has earned both his master's and bachelor's degrees from Panjab University (Chandigarh). He has acted as a resource person at several FDPs, MDPs and Workshops at various institutions.