

Mirbabaie, Milad; Brünker, Felix; Möllmann Frick, Nicholas R. J.; Stieglitz, Stefan

Article — Published Version

The rise of artificial intelligence – understanding the AI identity threat at the workplace

Electronic Markets

Provided in Cooperation with:

Springer Nature

Suggested Citation: Mirbabaie, Milad; Brünker, Felix; Möllmann Frick, Nicholas R. J.; Stieglitz, Stefan (2021) : The rise of artificial intelligence – understanding the AI identity threat at the workplace, *Electronic Markets*, ISSN 1422-8890, Springer, Berlin, Heidelberg, Vol. 32, Iss. 1, pp. 73-99,
<https://doi.org/10.1007/s12525-021-00496-x>

This Version is available at:

<https://hdl.handle.net/10419/287452>

Standard-Nutzungsbedingungen:

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

Terms of use:

Documents in EconStor may be saved and copied for your personal and scholarly purposes.

You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.

If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.



<https://creativecommons.org/licenses/by/4.0/>



The rise of artificial intelligence – understanding the AI identity threat at the workplace

Milad Mirbabaie¹ · Felix Brünker² · Nicholas R. J. Möllmann (Frick)² · Stefan Stieglitz²

Received: 22 December 2020 / Accepted: 24 August 2021 / Published online: 5 October 2021
© The Author(s) 2021, corrected publication 2022

Abstract

Artificial intelligence (AI) is being increasingly integrated into enterprises to foster collaboration within humanmachine teams and assist employees with work-related tasks. However, introducing AI may negatively impact employees' identifications with their jobs as AI is expected to fundamentally change workplaces and professions, feeding into individuals' fears of being replaced. To broaden the understanding of the AI identity threat, the findings of this study reveal three central predictors for AI identity threat in the workplace: changes to work, loss of status position, and AI identity predicting AI identity threat in the workplace. This study enriches information systems literature by extending our understanding of collaboration with AI in the workplace to drive future research in this field. Researchers and practitioners understand the implications of employees' identity when collaborating with AI and comprehend which factors are relevant when introducing AI in the workplace.

Keywords Artificial intelligence · IT identity · Identity threat · Information systems · Workplace

JEL classification O33

Introduction

The ongoing development of information technology (IT) enables organizations to introduce digital work as the new normal. Therefore, employees are facing new forms of work that might decrease personal interaction but increase interaction with IT. Nevertheless, these new ways of work

entail that individuals cannot do their jobs with the same values and convictions as they are used to. There is a constant change that might impact selfbeliefs constituting professional identity at work, i.e., the perception of one's role in the workplace. Experiencing a situation that contradicts one's identity might lead to a loss of self-esteem and thus to a threat to identity (Petriglieri, 2011). This might enforce actions designed to protect self-esteem correlated with identity (Craig et al., 2019) as emerging technologies have changed the landscape and experiences of a variety of professions (Frick et al., 2021). The digitization of the workplace emphasizes the demand for digital work as the new normal in organizations (Baptista et al., 2020; Frick & Marx, 2021). One major factor driving this discussion is the ongoing development of artificial intelligence (AI), which that can be described as “the ability of a machine to perform cognitive functions that we associate with human minds, such as perceiving, reasoning, learning, interacting with the environment, problem solving, decision-making, and even demonstrating creativity” (Rai et al., 2019, p. iii). In digital work, AI is applied for various functions, such as (managerial) decision making (Haesevoets et al., 2021), data analysis and prediction work (Grønsund & Aanestad, 2020; Marabelli et al., 2021), or (human-AI) collaboration

Responsible Editor: Xiao-Liang Shen

✉ Milad Mirbabaie
milad.mirbabaie@uni-paderborn.de

Felix Brünker
felix-bruenker@uni-due.de

Nicholas R. J. Möllmann (Frick)
nicholas.frick@uni-due.de

Stefan Stieglitz
stefan.stieglitz@uni-due.de

¹ Information Systems & Digital Society, Paderborn University, 33098 Paderborn, Germany

² Digital Communication and Transformation, University of Duisburg-Essen, 47057 Duisburg, Germany

(Brachten et al., 2020; Mirbabaie et al., 2020, 2021). Therefore, AI will change workplaces and professions persistently, potentially threatening the livelihoods of individuals whose jobs are taken over (Aleksander, 2017; Haenlein & Kaplan, 2019). However, AI might lead to value co-destruction when discrepancies between users emerge (Camilleri & Neuhofer, 2017). Furthermore, the use of AI could also support the development of uncertainty and invasion of privacy (Cheng et al., 2021). This negative phenomenon is often referred to as the dark side of AI, referring to how AI presents risks for individuals, organizations, and society (Alt, 2018; Grundner & Neuhofer, 2021; Wirtz et al., 2020). Nonetheless, the utilization of AI in organizations could not only eliminate or change current jobs but also create new areas of work, for example, within engineering, programming, or even in social domains (Acemoglu & Restrepo, 2018). There is ongoing hype about AI and its economic impacts (Selz, 2020). Although the public discussion about AI has turned more optimistic in recent years, the fear of AI eliminating current jobs still outweighs the possible opportunities for human-AI collaboration (Acemoglu & Restrepo, 2018; Aleksander, 2017; Dwivedi et al., 2019; Wang & Siau, 2019; Zhang & Dafoe, 2019).

Human-AI interaction reveals that individuals' perceptions of AI are based on different aspects. For example, salient cues, affordances, or collaborative interaction (Sundar, 2020; Wirtz et al., 2020) might affect individuals' emotions and, therefore, intentions toward AI (Shin, 2021). Employees establish an identity in relation to applied technology and their jobs. To adequately consider this phenomenon, we take on the perspective of Carter and Grover (2015), who introduce the term *IT identity* and define it as "the extent to which a person views use of an IT as integral to his or her sense of self" (Carter and Grover, 2015, p. 938). Introducing AI in the workplace may contradict employees' identification with their jobs and lead to resistance behavior such as *algorithm aversion*. Algorithm aversion describes a phenomenon in which, under the same conditions, employees prefer a human over algorithmic decision support (Dietvorst et al., 2015; Venkatesh, 2021). Craig et al. (2019, p. 269) describe this resistance as *IT identity threat*, defined as "the anticipation of harm to an individual's self-beliefs, caused by the use of an IT, and the entity it applies to is the individual user of an IT." Therefore, it is vital to understand the emergence of upcoming predictors influencing AI resistance based on IT identity threats as the application of AI is likely to alter jobs in organizations and thus might impact individuals' identities.

To contribute to reducing resistance to AI, it is crucial to broaden the understanding of identity threats caused by AI as unique technology. To minimize AI related threats towards the identity of employees, it is essential to position AI as a benign and supportive collaboration technology. We

argue that this is of great interest to information systems (IS) researchers and practitioners alike as the application of AI for generating business value will further increase, successively turning into key elements for enterprises (Dwivedi et al., 2019). Considering the social interactions between individuals and technology and its possible threat to identity, further investigations into IT identity threat are needed to understand this phenomenon (Craig et al., 2019). There is thus an urgent demand to conduct in-depth research on new forms of human-AI collaboration, especially on related consequences for employees in terms of attitudes and actions toward AI as well as psychological, emotional, and social aspects (Coombs et al., 2020). The continuing distribution of AI in electronic markets (Adam et al., 2020; Thiebes et al., 2020) therefore entails the pressing need for IS to investigate potential influences on the IT identity threat caused by AI. Based on these arguments, this study rests upon the following research question:

RQ: Which predictors influence the AI identity threat of employees in the workplace?

To answer this research question, we initially carried out a systematic literature review (SLR) following the latest methodological guidelines for literature reviews in IS (e.g., Okoli, 2015; Paré et al., 2015). We argue that the complexity as well as opportunities of AI and associated identities of employees in the workplace, as well as related threats, have not yet been adequately covered in the research. This descriptive procedure examines existing literature describing the current situation to synthesize research evidence based on scientific facts (Bear & Knobe, 2017; Bell, 1989; Grant & Booth, 2009). Building upon these findings, we derive a research model, including predictors for the AI identity threat of employees in the workplace, which was quantitatively evaluated using partial least square structural equation modeling (PLS-SEM) as a favorable approach for the assessment of multistage models (Fornell & Bookstein, 1982). As there are different interpretations of the appropriateness of PLS as a suitable SEM technique (e.g., Goodhue & Thompson, 2012; Hair et al., 2017; Marcoulides et al., 2009; McIntosh et al., 2014; Petter & Stafford, 2017), we followed the latest recommendations of Hair et al. (2019) to alleviate ascending concerns. We finally conducted post-hoc expert-interviews to evaluate the model and the identified predictors for the AI identity threat of employees in the workplace. Individuals thereby elaborated on the current state of the art and their experiences (e.g., descriptive procedure) (Bear & Knobe, 2017).

This paper contributes to theory and practice by extending our understanding of collaboration with AI in the workplace to drive future research in this field. Researchers will find the insights helpful in understanding the implications

of employees' identity when collaborating with AI in enterprises. By providing a theory-based framework, scholars will assess which predictors cause AI identity threat in the workplace. Practitioners will be able to comprehend which factors are particularly relevant when introducing AI for collaborative purposes. Readers will realize that employees perceive identity fears when AI is increasingly applied. Human-AI collaboration is more likely to be successful when possible threats are understood and overcome. We believe this study will be valuable to researchers, practitioners, and society for understanding and overcoming obstacles when collaborating with AI. Hence, this article extends the IS literature by updating our knowledge on identity and related threats in the context of AI in a collaborative working environment and how predictors are interconnected.

Theoretical background

The need for AI in the workplace

AI is increasingly being augmented in electronic markets, triggering a widespread acceptance in organizations across industrial boundaries and transforming the global economy (Adam et al., 2020; Guan et al., 2020; Thiebes et al., 2020). Therefore, AI is considered an integral part of business strategy and organizational decision making (Cheng et al., 2020a, b; Shrestha et al., 2019), thus making it a key element for generating business value (Dwivedi et al., 2019). As a ubiquitous concept (Siau & Wang, 2018), AI consists of multiple subfields and dimensions (i.e., think like a human, think rationally, act like a human, and act rationally) (Ruszel & Norvig, 2016), but without evolving into a consistent definition (Duan et al., 2019). AI is usually associated with human intelligence, but society is facing the question of how machines are able to reach this kind of intelligent behavior (Neuhofer et al., 2020), yielding a three-dimensional categorization: narrow AI, general AI, and superintelligence (Batin & Turchin, 2017). Narrow AI covers self-learning approaches that outperform humans on specific, narrow tasks. General AI explains self-learning comparable to the intelligence of humans. Superintelligence, hypothetically, is thought to exceed humans in all aspects. Most applied systems in organizations are considered narrow AI as they focus on particular work-related tasks (Batin & Turchin, 2017). AI is believed to fundamentally change the working environment and the way people work (Bednar & Welch, 2020), spreading across industries (Wang & Siau, 2019) with potential applications in almost every field (Barredo Arrieta et al., 2020). However, among the changes in working environments and models, AI possesses unique issues. Since AI is still implemented by humans, systems might contain certain biases as individual backgrounds and experiences

(i.e., development of heuristics) are reflected. Some of these could lead to bigger or more frequent mistakes made by the AI (Wirtz et al., 2020). Moreover, not every AI model is explainable due to its sophisticated structure. It thus represents a *black box* for humans that prevents understanding certain decisions and leads to increased uncertainty (Venkatesh, 2021). In the context of generating predictions involving humans, this negatively affects the privacy perceptions of individuals (Cheng et al., 2021). While there are arguments that highlight the bright side of AI, such as improvements to efficiency or cost reduction, aspects of the dark side of AI may have a stronger effect on the perceptions of employees toward AI (Grundner & Neuhofer, 2021). Thus, a simple economic decision such as cost reduction based on decreasing the headcount in an organization might lead to the fundamental anxiety of being replaced by AI (Złotowski et al., 2017). The current generation of narrow AI in enterprise is still new and multi-faceted. There is widespread speculation about collaborative capabilities and relevance, and many employees only have a vague picture of collaboration with AI in their workplaces (Kühl et al., 2019). Research has demonstrated that human-AI interaction is able to shape processes more effectively and enhances the individual performance of employees. Employees are supported in the decision-making process (Dellermann et al., 2019; Metaxiotis, 2000), strategic decisions are facilitated (Aversa et al., 2018), and human-AI collaboration frees humans from repetitive tasks, helping them embrace strong economic potential (Yang & Siau, 2018). A recent study employed an AI-based system within the incident management process of an IT department collaborating with help desk employees on the hitherto manual categorization process (Frick et al., 2019). The study illustrated that over 90% of incidents were properly classified. This is not only superior to humans but also frees individuals from repetitive tasks. Another study proved that collaboration with AI in the form of virtual assistants (VAs), computer-based support systems, is capable of supporting employees during the solution of work-related tasks (Brachten et al., 2020). The findings indicate that, first, the collaborative execution of tasks is more efficient and, second, VAs decrease the load, illustrating that collaboration also reduces the perceived workload of employees in the workplace. Furthermore, Mirbabaie et al. (2020) examined social identity, i.e., the identification of employees with team members, and extended self, i.e., the incorporation of possessions into one's sense of self, when humans work with VAs in teams. The authors derived a new concept, *virtually extended identification*, elaborating that individuals who identify themselves with (virtual) team members are also more likely to identify with the technology as a part of their extended selves and vice versa. This intertwining highlights that research needs to adjust its understanding

of identification with AI and that different collaborative settings, such as identity and related threats, need to be examined.

On the one hand, AI is considered an engine for productivity and progress; on the other hand, AI entails societal upheaval (Yang & Siau, 2018). It is not only of particular interest to assess how to drive business success and value by applying AI; there are several theoretical and practical strategies (Adam et al., 2020; Frick et al., 2019, 2020; Selz, 2020). However, it is especially vital to examine whether employees establish a certain identity with AI (Mirbabaie et al., 2020) and which predictors influence AI identity threat. A successful application for collaborative purposes to generate business value is thus only achievable when employees somewhat identify themselves with AI and perceive AIs as equal collaborative partners and elemental parts of their work.

IT identity and related threats

This paper follows the perspective of concept identity as the “answer to the question ‘Who am I?’ in relation to a social category or object” (Carter and Grover, 2015, p. 933). A person always only holds one self-concept, while it is possible to hold multiple identities (Stets & Burke, 2000). Whereas the *collective level* of identity explains how identity is formed from a membership in social groups (Stets & Burke, 2000), the *individual level* describes how the connections and relationships of people influence their identity and, subsequently, behavior toward others (Burke & Stryker, 2016). In this context, *role identity* (e.g., work, sports, parents) is verified when people act according to the internalized expectations toward a specific role. *Person identities* are verified when people perform in ways that are aligned to values and norms that differentiate themselves as unique individuals. Last, *material identities* are verified when people are able to control or master a material object with which they are interacting (Carter and Grover, 2015). However, people do not only verify their identity based on their experience among role, person and material identity. Individuals also face contradictions to their self-beliefs that may result in experiencing potential harm to one’s identity (Petriglieri, 2011). Thus, “when an experience contradicts identity, individuals experience a loss of self-esteem and take action to preserve the self-esteem associated with identity” (Craig et al., 2019, p. 265). Those actions may yield into resistance behavior or a change of the current identity concept. Furthermore, the scholars describing the nature of the identity threat as harm to the meanings, value or enactment of an identity (Craig et al., 2019; Petriglieri, 2011). This potential harm to an individual’s identity may affect role, person or material identity. While the concepts of role and person identity focus on group processes and group identities, the material identity is more connected with individual behavior and thinking

(Boudreau et al., 2014; Gong et al., 2020). Considering the perspective of identity in relation to the question “Who am I?”, we follow the conceptualization of Carter and Grover (2015), who understand *IT identity* as a new form of material identity. IT identity can be defined as “the extent to which a person views use of an IT as integral to his or her sense of self, where a strong IT identity represents identification—‘use of the [target IT] is integral to my sense of self (who I am)’—and a weak IT identity represents dis-identification—‘use of the [target IT] is completely unrelated to my sense of self (who I am)’ (Carter and Grover, 2015, p. 938). The authors state that in the context of IT identity, IT can be defined as any unit of technology that allows a user to consciously interact with it to produce, store, and communicate information and that is accessible at any time or place.

However, introducing and using a new technology might not yield acceptance. The identification with IT might be beneficial but entails certain drawbacks, separated into four categories of identity: IT identity, absent IT identity, anti-IT identity, and ambivalent IT identity (Carter et al., 2019). IS research already covers single factors of resistance to IT, e.g., the fear of losing human uniqueness (Stein et al., 2019), the deskilling of professionals (Boudreau et al., 2014), information interruption of emotional exhaustion (Cheng et al., 2020a, b), the protection of a certain threatening event (Sun et al., 2020), and the possibility of unemployment or the chance of losing safety (Złotowski et al., 2017). Considering the social interactions between individuals and technology and its possible threat to identity has mainly been neglected in IS research (Craig et al., 2019).

Therefore, scholars have introduced the concept of IT identity threat as “the anticipation of harm to an individual’s self-beliefs, caused by the use of an IT” (Craig et al., 2019, p. 269). The need for examining the threat of IT to individuals’ identities becomes apparent when observing the changing landscape of digital collaboration. Recent research has started to investigate IT identity by considering technology such as Excel or smartphones (Carter et al., 2020b). This step has been fundamental to strengthening the understanding of IT identity. However, regarding new forms of collaboration in the workplace, IT, or specific IT features such as Excel calculations, are often replaced by AI systems that support, for example, decision making or data analysis (Mirbabaie et al., 2020). Thus, analyzing IT identity by using traditional IT might not be sufficient to understand identification with technology such as AI in the workplace. Thus, research elaborating the role of AI as a technology that breaks the boundaries of historic IT is urgently needed. For example, Alahmad and Robert (2020) revealed that the identification with AI impacts job performance. Focusing on human-AI collaboration in organizations, we ask the question “Who am I as a professional when collaborating with AI in the workplace?” and define AI identity, leaning

on existing explanations (Carter and Grover, 2015), such as “the extent to which individuals perceive the collaboration with AI in the workplace as an indispensable component of themselves.” While the identity threat has been researched in the context of different technologies (Craig et al., 2019; Stein et al., 2019), the unique and novel characteristics of AI in the workplace make it indispensable to investigate AI’s role in identity threat.

Research approach

Since the transfer of the concept of IT identity and related threats into the realm of AI has not been adequately covered by extant research, we performed an SLR to identify relevant literature and reveal interpretable patterns and theories (Paré et al., 2015). Existing conceptualizations and propositions (Paré et al., 2015) serve as a theoretical foundation to derive a research model predicting AI identity in the workplace. We further quantitatively evaluated our research model using PLS-SEM, enabling us to explain causal relationships of identified predictors of AI identity threat (Hair et al., 2019). Finally, to examine whether the identified predictors are really relevant to AI identity threat, we conducted semi-structured interviews with experts who are familiar with AI in their workplaces. To better provide an overview of the applied methods, Fig. 1 shows the distinct steps of the procedure.

Systematic literature review

An SLR is especially helpful for identifying existing knowledge about a topic, including related gaps, by searching for relevant articles using keywords in scientific databases (Fink, 2013; Webster & Watson, 2002). Since we use the SLR to emphasize our contribution to knowledge based on an interpretable pattern from existing literature (Fink, 2013; Webster & Watson, 2002), this is considered to be a descriptive process describing the current state of the research domain by relying on scientific facts (Bear & Knobe, 2017) and further transferring it to an emerging topic. We analyzed the literature according to evidence of predetermined qualitative themes (e.g., IT identity and related predictors), leading to deductive results (Bandara et al., 2015). Ali and Birley (1999) explain that within this procedure, “the scientist formulates a particular theoretical framework and then sets about testing it.” We used a priori coding themes from our studied phenomenon (Ali & Birley, 1999). This theoretical sensitivity is particularly helpful as codes can be derived from, for instance, scientific definitions or established constructs (Ryan & Bernard, 2003; Strauss & Corbin, 1990). Following the literature review process (vom Brocke et al., 2009, 2015), we defined our research scope based on the taxonomy of literature reviews (Cooper, 1988). We were interested in research focusing on the phenomenon of identity, IT identity, identity threats, and IT resistance in relation to the workplace.

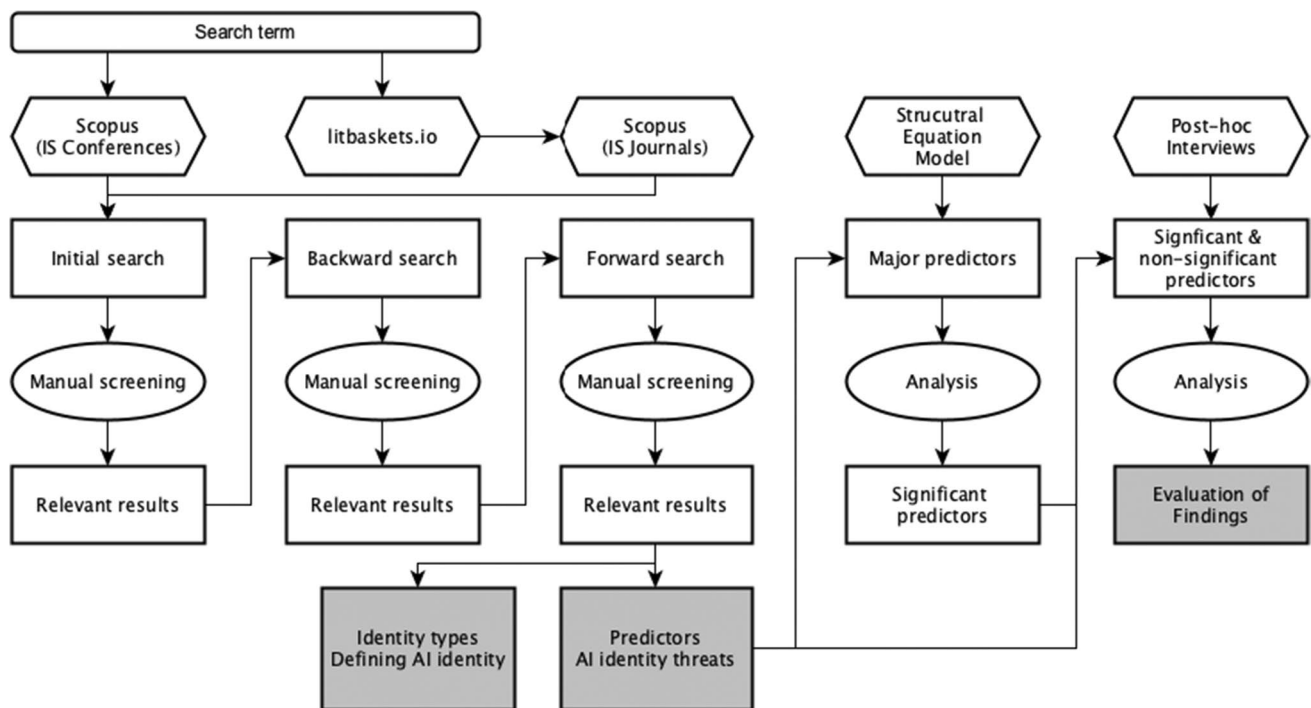


Fig. 1 Procedures of the applied methods

The literature search was conducted using litbaskets.io, an IT artifact with the aim of assisting IS researchers in retrieving relevant literature from major scientific sources (Boell & Wang, 2019). A search string was created with the ISSN numbers of the selected outlets, which was used in Scopus's advanced search, making it possible to search across all indexed scientific sources (Boell & Wang, 2019). Litbaskets offers the possibility to set different filters and size restrictions to limit the search or exclude certain sources or publications. We deliberately chose the 154 essential IS journals (*basket of eight* and other high-ranked outlets, such as *Information Systems Frontiers* and *Electronic Markets*) as we wanted to focus on substantial and high-quality articles. Since litbaskets focuses on IS journals but omits conferences, we extended the literature search by selecting the elementary IS conferences (AMCIS, ECIS, ICIS, PACIS, HICSS, and *Wirtschaftsinformatik*) manually via Scopus. Our literature search acknowledged peer-reviewed articles. Less relevant sources, e.g., editorials or commentaries, were excluded. We carried out a full text and metadata search and deliberately did not limit it to metadata only as this might not contain the search term, and further narrowing down the possibility of overlooking relevant publications. The research procedure considered articles published up until May 2020. We used the following query for our fulltext search:

((“identity threat”) OR identity OR (“IT identity”) OR (“AI identity”) OR (“IT resistance”)) AND (AI OR (“artificial intelligence”) OR (robot*) OR (“disruptive technology”) OR (“digital transformation”) OR (“information system”) OR (“information technology”) OR (“digitali*ation”)) AND (task OR work* OR job OR profession* OR career OR firm OR organi*ation* OR company OR business OR office OR enterprise OR corporation* OR association)

To obtain thorough results and provide an overview on the current state of research, we carried out several exemplary literature searches prior to the execution of our SLR. This served us in finding the most promising results to identify predictors related to AI identity threat. Our final search string covered three major sections. First, we used terms that covered literature related to identity and possible threats. Combinations of *IT* and *identity* are frequently used in extant research. Second, phrases linked to AI and associated concepts and technologies were included. For example, we added *digital transformation* and *digitali*ation* to our search query as AI is considered as key factor in this advancement (Frick et al., 2021). Third, different appellations for organizations and workrelated contexts were added. Depending on each research focus and authors' preferences, different terms such as *organization*, *company*, or *enterprise* were used. Parentheses nested clauses, Boolean expressions

linked individual nomenclatures, quotation marks combined terms that must appear next to each other, and asterisks marked different spellings (such as in American and British English).

After the initial search was finished, we carefully read the title, abstract, and keywords of each publication to determine its relevance to our research questions. Our selection was guided by the following questions: How can IT identity be described in the workplace? Which negative effects for employees result from the application of IT? Which factors influence identity threat in organizations? Since we wanted to adapt theoretical insights from IT contexts to the area of AI, we focused on articles dealing with the application of IT in the workplace and associated threats. We excluded articles, for instance, if they only dealt with the technical implications of technology. To achieve a comprehensive review, we next performed a backward search. Further literature was identified by collecting every reference of the bibliographies of all the papers from the initial search. We included references to other journal or conference publications and excluded non-scientific sources, such as web pages or business reports. To determine the relevance according to our research questions, we conducted a similar approach as within the initial search: we read the title, abstract, and keywords, which was followed by categorization according to theoretical foundations. The last step of the literature review was a forward search to identify additional relevant literature. We acknowledged every paper that was identified during the previous initial and backward searches and that had been cited by other research after its initial publication.

The execution resulted in 49 relevant articles. We screened 5,649 articles, of which 21 (of 326) were found to be relevant during the initial search, 10 (of 2,057) via the backward search, and, finally, 18 (of 3,266) relevant publications were retrieved during the forward search. Table 1 outlines the number of search results per search type. No articles yielded by our search terms were published before 1998, and the number of publications has risen since. For example, in 2018, there were 5 (10.2%) publications, followed by 9 (18.4%) in 2019. The constant growth of research and publications reflects not only the pressing need for further studies but also represents

Table 1 Number of search results per type

Search type	Number of results	Number of relevant results
Initial search	326	21
Backward search	2,057	20
Forward search	3,266	18
Total numbers of articles	5,649	49

the salience and legitimacy of this research area. Furthermore, from the total of 49 articles, 36 (73.5%) are in journals, and 13 (26.5%) are conference publications. The majority of articles were published at the International Conference on Information Systems (5, 10.2%) followed by *Computers in Human Behavior*, *European Conference on Information Systems*, *European Journal of Information Systems*, and *Information and Organization*, with three articles each.

To understand how AI can be explained in the context of identity in the workplace (e.g., AI identity), we clustered the articles along the different identity types. Overall, we found 36 articles that dealt with identity, of which 15 (41.7%) dealt with identity in general, 16 (44.4%) researched professional identity, and the minority considered IT identity (5, 13.9%). There were no papers that dealt with the concept of AI identity. Current IS research on identity can be distinguished as follows (cf. Table 2): identity, which typically asks the question “Who am I?” (Alvesson et al., 2008; Lamb & Davidson, 2005; Park & Kaye, 2019), explains the social role and/or influence of individuals (Boudreau et al., 2014; D’Mello & Eriksen, 2010; Elbanna & Linderoth, 2015; Sime & Themelis, 2020). Professional identity asks, “Who am I as a professional” (Chreim et al., 2007), refers to the self-perception of an employee in the workplace (Jussupow, 2018; Jussupow et al., 2018), and is defined as “an individual’s selfdefinition as a member of a profession and is associated with the enactment of a professional role” (Chreim et al., 2007). IT identity specifies how humans identify with information technology and is interpreted as “the extent to which an individual views use of an IT as integral to his or her sense of self” (Carter and Grover, 2015).

Model development

Besides obtaining an overview of current identity types, we analyzed the papers for possible identity threats and their type of influence. In total, we found 22 papers illustrating 24 predictors for identity threat. Since this research focuses on the AI identity threats experienced by employees, we were specifically interested in predictors that might cause individual identity shifts in the workplace. Professional self-image consists of having status and value (Alvarez, 2008) and is, besides technology, altered by certain factors (Jussupow et al., 2018). The identified predictors were thus analyzed regarding their potential strength of influence on the identity threat. If an individual faces threat to its identity, it may lead to identity protection responses that could lead to several effects (Jussupow et al., 2018). For instance, resistance behavior, refusing to engage with technology (Nach, 2015), and forming a certain anti-identity (Carroll & Levy, 2008) may arise as protection response behavior to reduce incoming identity threats by AI. Individuals might even emotionally regulate their threatened identities through, i.e., increasing work volume, meditating, or crying (da Cunha & Orlikowski, 2008). Thus, understanding identity threats caused by AI is important to resolve harmful effects that are rooted in the introduction of AI at the workplace. To this end, we found six predictors that might cause AI identity threats to employees in the workplace.

We further used the threat sources of the identity threat framework to cluster the final predictors (Craig et al., 2019). First, intergroup conflict explains the reputation and self-beliefs within a social group. Conflicts within, for example, a team in the workplace may result in the loss of resources, status, or prestige. Second, verification prevented describes the personal perception and inspection of self-beliefs initiated or influenced by technology. Third, meaning change

Table 2 Articles assigned to different identity types

Type	Explanation	Referenced by
<i>Identity</i>	The individual’s perception of his/her role in the social community	(Alvesson et al., 2008; Boudreau et al., 2014, 2016; Craig et al., 2019; D’Mello & Eriksen, 2010; Elbanna & Linderoth, 2015; You & Robert Jr., 2018; Hoffman & Novak, 2018; Israeli, 2019; Jensen et al., 2009; Nach, 2015; Park & Kaye, 2019; Sime & Themelis, 2020; Utesheva et al., 2016; Vaast et al., 2013)
<i>Professional identity</i>	The individual’s perception of his/her role in the workplace	(Aboud, 2020; Abouzahra et al., 2015; Alvarez, 2008; Bernardi & Exworthy, 2020; Brooks et al., 2011; Daskalopoulou et al., 2019; Geertshuis & Liu, 2016; Hicks, 2014; Israeli, 2019; Jussupow, 2018; Jussupow et al., 2018; Karsten & Laine, 2007; Lamb & Davidson, 2005; Stein et al., 2013; Svejvig & Jensen, 2012; Teubner, 2007; Walsham, 1998)
<i>IT identity</i>	The individual’s perception of IT being an integral part of oneself; feeling related and dependent	(Carter and Grover, 2015; Gong et al., 2020; Israeli, 2019; Ogbanufe & Gerhart, 2020; Park & Kaye, 2019)

is triggered by modifications of work-related tasks. Thus, changes in tasks alter the meaning of the job itself, which might not be consistent with the professional identity of an employee. Table 3 outlines the classification of the six predictors, along their threat sources, and presents explanations and exemplary influences.

Loss of status position and threats to job security can be categorized as intergroup conflicts since both factors have a considerable impact on perception within social groups in the workplace. Introducing AI at the workplace may enhance the sense of loss of status and job security by overtaking certain tasks or responsibilities and therefore threaten one’s established identity. Złotowski et al. (2017) found that technology that is capable of solving employees’ tasks leads to an increased perception of threat to job security. Likewise, Craig et al. (2019) argue that IT that substitutes distinct parts of a job might lead to a reduction of power or prestige associated with that status position. In this context, Jussupow et al. (2018) argue that AI might act as an individual, direct threat to the social position of an employee. These threats might lead to reduction of power and prestige in the workplace. Therefore, we formulate the following hypotheses:

H1a: Threat to job security has a positive effect on AI identity threat in the workplace.

H1b: Loss of status position has a positive effect on the AI identity threat in the workplace.

Loss of skills/expertise and changes to work can be described with verification prevented as, due to the changes in work-related tasks, self-beliefs are validated. Jussupow et al. (2018) argue that the threat to skills/expertise is rooted in the usage of technology. This might lead to a decreased need for specialized skills and knowledge by employees (Hicks, 2014). Thus, one’s identity that is built on the personal skills and expertise may be vulnerable to new technology such as AI that need to quantitate certain tasks. Therefore, AI might be capable of changing the perception of one’s own skillset by exposing personal (performance) weaknesses. Thus, introducing a new technology such as AI is often linked to changes in the workplace (Craig et al., 2019). These new changes to work may evoke feelings such as restlessness or disengagement that lead to a lack of involvement and therefore to threat to one’s identity. Therefore, we derive H2a and H2b:

H2a: Loss of skills/expertise has a positive effect on AI identity threat in the workplace.

H2b: Changes to work have a positive effect on AI identity threat in the workplace.

Loss of autonomy and loss of controllability are covered by meaning changes as technology-induced changes might

Table 3 Possible predictors and hypotheses of AI identity threat

Threat source	Predictor (ref. by)	Explanation	Exemplary influence
<i>Intergroup conflict</i>	Threat to job security (Craig et al., 2019; Prester et al., 2019; Złotowski et al., 2017) Loss of status position (Israeli, 2019; Jussupow et al., 2018)	Professional’s perception of her own secured employment in the workplace Professional’s perception of the damage to status induced by technology	Reduction of power and prestige, less validation of professional role, limiting flexibility Frustration, helplessness, grief, difficulties in communication
<i>Verification prevented</i>	Loss of skills/expertise (Alvarez, 2008; Hicks, 2014; Jensen et al., 2009; Jussupow et al., 2018) Changes to work (Craig et al., 2019; Hicks, 2014; Jussupow et al., 2018)	Professional’s perception of the harm to knowledge induced by technology Professional’s perception of the impact of changes in the workplace	Diminishing professional value, sense of deskilling, ignorance Restlessness, disengagement, lack of involvement, feeling less secure in professional position
<i>Meaning change</i>	Loss of autonomy (Jensen et al., 2009; Jussupow et al., 2018; Prester et al., 2019) Loss of controllability (Nach, 2015; Park & Kaye, 2019; Schweitzer et al., 2019; Stein et al., 2013) AI identity (Carter and Grover, 2015; Craig et al., 2019)	Professional’s perception of liberties over conditions, processes, or procedures in her area of responsibility Professional’s perception of control over conditions, processes, or procedures in her area of responsibility Professional’s perception of the extent to which the collaboration with AI in the workplace is an indispensable component of herself	Missing engagement with processes and tasks, constantly feeling challenged Emotional regulation (e.g., anger, crying, meditating, leaning back), lacking sense of order and continuity Feeling related, dependent, wanted, and needed

significantly alter professional responsibilities. This may lead to an increased threat to the identity as professional responsibilities might be strongly linked to one’s identity at the workplace. In this context, Schweitzer et al. (2019) identify distinct relationships with AI-based devices. The scholars reveal the fear of losing control over one’s digital self when interacting with a smart device. Furthermore, research indicates that technology may impact the control and autonomy of daily and work life as well. For example, Park and Kaye (2019) describe the renunciation of technology as a strategy to regain control of daily life. The scholars argue also that technology could be part of one’s self and therefore influences the individual identity either in a positive or negative way. Likewise, Prester et al. (2019) emphasize the close relationship between digital technologies, workplaces, and human identity in the context of professional autonomy and maintaining the self. Furthermore, Nach (2015) describes an upcoming threat by IT when an individual appraises a situation as uncontrollable. If an individual perceives the situation as controllable, they deploy strategies to neutralize the potential threat by an IT. However, the application of AI encompasses the capabilities of reducing the employee’s perceived autonomy and controllability in the workplace. This emphasizes the potential relationship between autonomy and controllability with an AI identity threat. Thus, the following hypotheses are derived:

- H3a: Loss of autonomy has a positive effect on AI identity threat in the workplace.
- H3b: Loss of controllability has a positive effect on AI identity threat in the workplace.

Besides the predictors identified by the conducted SLR, it can be assumed that the concept of AI identity, as previously defined, has a major impact on the AI identity threat itself. According to Carter and Grover (2015), individuals identify positively or negatively with a distinct IT. This assumption can be transferred to AI as the object of research. When employees perceive that AI is an integral part of themselves and are committed to collaborating with AI to accomplish specific work-related tasks, this may result in the technology not being regarded as a hazard (Grundner & Neuhofer, 2021; Złotowski et al., 2017). However, a negative identification with AI may support the perceived threat caused by AI in the workplace (Alahmad & Robert, 2020; Craig et al., 2019). This prevailing attitude of employees is crucial to consider when broadening the understanding of AI identity threat. Thus, we derive the following hypothesis:

- H4: AI identity has a negative effect on AI identity threat in the workplace.

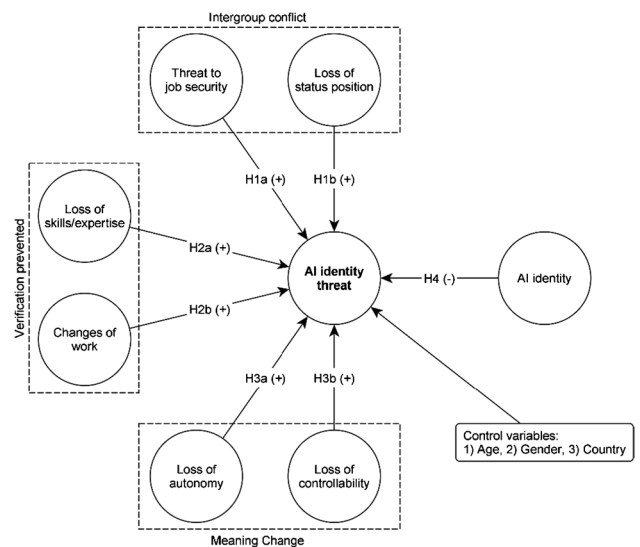


Fig. 2 Research model including constructs and hypotheses as developed from the literature

To put the hypothesis of the specific predictors into context, we conceptualize a research model (Fig. 2 and 3) that allows further analysis of the AI identity threat and the identified predictors.

Expert interviews

The SLR is suited for identifying predictors of AI identity threat in the workplace. We therefore adapted findings from existing research in which AI might not have been adequately covered. We conducted post-hoc interviews to

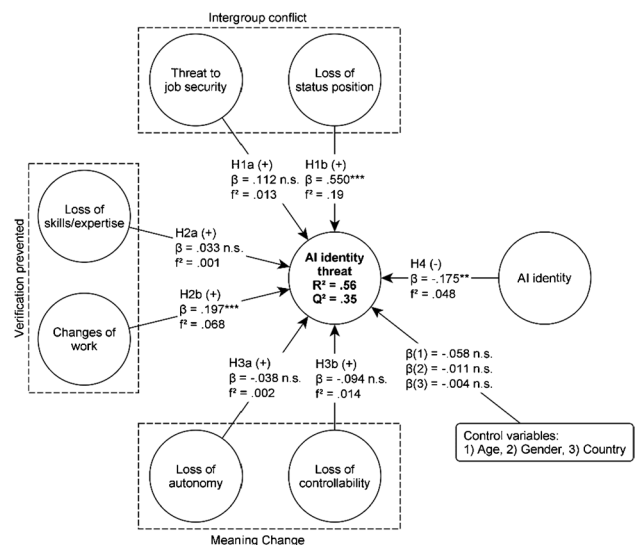


Fig. 3 Research model with results (N=303). *p ≤ 0.05; **p ≤ 0.01; ***p ≤ 0.001

validate whether the identified predictors are really relevant in our research context.

Expert interviews are sufficient for retrieving knowledge from qualified experts (Kvale & Brinkmann, 2009) and are especially fruitful for less explored research areas (Bogner et al., 2009). Experts possess specific domain expertise (Meuser & Nagel, 2009); in our case, these are individuals who have participated in or initiated an AI-induced change process in the workplace. To obtain a holistic picture, we chose participants working at the management level to broaden our understanding of the research field (Bogner et al., 2009). We followed the suggestions of Creswell and Creswell (2018) and included between three and ten individuals for our qualitative procedure. In total, we conducted six interviews with the male participants. Experts were between 24 and 38 years old ($SD = 4.92$; $M = 33.66$). The experts' characteristics can be retrieved from the Appendix (Table 8). We followed an open interview technique, using a semi-structured approach. Experts were given the opportunity to elaborate on their subjective beliefs but were supported by a prefixed guideline with essential questions (Meuser & Nagel, 2009; Qu & Dumay, 2011). The interviews started with welcoming the participants and describing the interview process, including a short briefing of the study. In the first phase, we obtained the interviewees' characteristics, which aided us in understanding their working environments. The next phase included questions on AI in the workplace; we provided a definition on AI to establish the same level of knowledge among all participants throughout the interviews. The third phase served to validate our derived research model and the identified predictors for AI identity threat in the workplace. In the last phase, experts had the opportunity to provide additional input or ask further questions. We concluded with a short debriefing. Since we were interested in the experts' opinions on the model and predictors rather than their gestures or facial expressions, we used paraphrasing as suggested by Schilling (2006). We limited the data by deleting irrelevant words or formulations to form short and concise sentences that led to generalized explanations or interpretations. We further applied open coding using in-vivo or with simple phrases (second order themes) and summarized them under the identified predictors (first order themes) (Gioia et al., 2013).

Quantitative data collection

To determine which of the identified factors impact AI identity threat in the workplace, we used a quantitative approach for validating the derived hypotheses with a large population (Creswell & Creswell, 2018). Since we were not able to build upon theoretical foundations for every factor used in our research model, we needed to develop and validate

constructs within a pre-study. The evaluated items, combined with measures adapted from existing literature, were used within the subsequent main study to test our developed research model.

Measurements and survey

We developed items for loss of status position and changes to work and evaluated them using a pre-study. Example items of experiences of loss of status position are "the introduction of AI will reduce my competences" and "by the introduction of AI, I am limited in my possibilities." Changes to work included items such as "the introduction of AI increases my area of responsibility" and "by the introduction of AI, I am responsible for more tasks." Extant research takes the standpoint that the introduction of new IT raises uncertainties, threats, and fears (Hirschheim & Newman, 1988; Laumer, 2011; Silva et al., 2016). Reducing and overcoming potential inhibitors is therefore especially crucial to avoid resistance behavior and an unfavorable climate for change (Bouckenooghe et al., 2009; Frick et al., 2021; Krovi, 1992). We argue that formulating the items using "the introduction of AI" is beneficial as anxieties (i.e., loss of status position and changes to work) are foremost observed prior to or during introduction processes (Joshi, 1991; Kim & Kankanhalli, 2009; Meissonier & Houzé, 2010).

We used a seven-point Likert scale ranging from "strongly disagree" to "strongly agree" to survey the items. In total, 91 participants started the questionnaire, and $N = 68$ respondents completed the survey. We screened the data manually for anomalies and suspicious responses (i.e., very short processing times and similar or identical answers) but did not need to exclude any further participants. The respondents were between 18 and 52 years old with a mean age of 32.3 ($SD = 10.3$), of which 22 (32.4%) were female and 46 (67.6%) were male. The results were tested for reliability using factor analysis. Loss of status position resulted in an overall Cronbach's alpha value of 0.882 ($M = 1.79$; $SD = 0.72$), and changes to work yielded a Cronbach's alpha of 0.864 ($M = 3.16$; $SD = 0.90$), indicating high reliability for the constructs. The evaluated scales were used within the following survey.

The main study was conducted to validate our research model. Besides demographic data, which were used as control variables, we adopted and modified constructs from previously validated instruments and applied the evaluated, self-developed items to ensure the high accuracy of the measures. The items are listed in Table 5 (see Appendix). All items were surveyed on a seven-point Likert scale ranging from "strongly disagree" to "strongly agree." Threat to job security was adapted from Hellgren et al. (1999), who analyzed job insecurity as an influencing factor on employee attitudes and well-being. Loss of skills/expertise was derived

from the Jussupow et al. (2018) conceptualization of professional identity threats in the workplace. Loss of autonomy as well as loss of controllability was based on Breugh (1985), who developed instruments to capture different aspects of work autonomy in organizations. AI identity was measured using items from Carter (2012), who proposed measures for IT identity, including the items of dependence, emotional energy, and relatedness (i.e., feeling attached, having endurance, and being linked to IT). AI identity threat was adapted from Craig et al. (2019), who determined an operational measure for IT identity threat. AI identity and AI identity threat were originally specified as second order constructs; we adapted them as first order constructs. Carter et al. (2020a) observed that first- and second-order models of IT identity are statistically equivalent and provide nearly identical fit statistics. Furthermore, the evaluation of higher order reflective constructs tends to be challenging and might not be valid in terms of their prediction perspective, e.g. (Lee & Cadogan, 2013; Sarstedt et al., 2016). Furthermore, we were interested in developing first order constructs to serve as a basis for future studies combining all relevant aspects as a set of conceptually distinct variables (Carter et al., 2020a, b; Hair et al., 2019).

Participants were recruited using prolific.co, a platform specifically designed to acquire participants for online surveys (Palan & Schitter, 2018). Participants were selected according to certain conditions: individuals needed to speak English fluently as the survey was presented in English. In addition, individuals needed to be part- or full-time employed and work in for-profit or non-profit organizations or in the local, state, or federal government. Furthermore, as we were concerned with AI, participants needed experience with AI in their private lives or in the workplace.

Descriptive statistics

Overall, 343 subjects participated in our survey, of which $N = 303$ finished the study properly. Again, we manually screened the data for anomalies regarding short processing times and suspicious responses with similar or identical answers. However, no answers needed to be removed from the dataset. Table 4 shows the ages of the respondents as being between 20 and 68 years old with a mean age of 39.1 ($SD = 10.1$). Gender was almost equally distributed. Two hundred and nine subjects lived in the UK (69.0%), followed

by 15 from Portugal (5.0%), and 13 each (4.3%) from Italy and Spain. Participants worked in consumer goods (54, 17.8%), research and education (44, 14.5%), healthcare (36, 11.9%), industry (36, 11.9%), and IT (34, 11.2%). Most participants worked as regular employees (162, 53.5%) followed by group/team leaders (75, 24.8%) and heads of department/subdivision (45, 14.9%). The comprehensive descriptive statistics can be found in Table 5.

PLS-SEM approach

The validation of our research model is based on PLS-SEM, which is particularly appropriate for multistage models containing diversified constructs, indicators, and relationships (Hair et al., 2011; Ringle et al., 2012; Sarstedt et al., 2016). To achieve significant levels of statistical power (Hair et al., 2011), PLS-SEM requires a minimum sample size, which is determined by multiplying the total number of paths directed at specific latent constructs by 10 (Hair et al., 2011; Marcoulides et al., 2009). We met this requirement with $N = 303$ participants. Since the construct indicators in our model are reflective measurements caused by latent variables (Churchill, 1979), we used consistent partial least square (PLSc) as a more robust method compared to traditional PLS approaches (Dijkstra & Henseler 2015). We calculated the PLS algorithm using a path weighting scheme with 300 iterations and 10–7 as the stop criterion. Bootstrapping was performed with a two-tailed, bias-corrected, and accelerated (BCa) confidence interval method with 4,999 subsamples (Henseler et al., 2016). Blindfolding was conducted with an omission distance of seven. SmartPLS (v. 3.3.2) (Ringle et al., 2020) was used for the PLSSEM analyses, and jamovi (v. 1.2.27.0) was used for descriptive statistics.

Results

In this section, we present the measurement and structural model analysis of our research model, followed by the calculation of group differences based on the latest considerations for the model development process by Hair et al. (2019).

Measurement model analysis

We initially examined the indicator loadings and removed items with values below the threshold of .708 (Hair et al., 2011) to achieve items with sufficient reliability (Fornell & Larcker, 1981; Hair et al., 2019). Internal consistency was ensured by measuring Cronbach's alpha, composite reliability, and Rho_A , resulting in sufficient values above 0.7 (cf. Table 6) (Diamantopoulos et al., 2012; Dijkstra and Henseler 2015; Hair et al. 2019). Convergent validity was estimated by assessing the average variance extracted (AVE)

Table 4 Descriptive statistics (age)

N	303
Mean	39.1
Median	37
Minimum	20
Maximum	68

Table 5 Descriptive statistics (gender, country, company, job)

	Counts	% of Total	Cumulative %
Gender			
Male	151	49.8%	49.8%
Female	152	50.2%	100.0%
Country			
Belgium	2	0.7%	0.7%
Canada	2	0.7%	1.3%
Cape Verde	1	0.3%	1.7%
Chile	1	0.3%	2.0%
Denmark	1	0.3%	2.3%
Estonia	2	0.7%	3.0%
Finland	3	1.0%	4.0%
France	1	0.3%	4.3%
Germany	3	1.0%	5.3%
Greece	4	1.3%	6.6%
Hungary	2	0.7%	7.3%
Italy	13	4.3%	11.6%
Japan	2	0.7%	12.2%
Mexico	3	1.0%	13.2%
Netherlands	3	1.0%	14.2%
Poland	9	3.0%	17.2%
Portugal	15	5.0%	22.1%
Spain	13	4.3%	26.4%
Sweden	1	0.3%	26.7%
United Kingdom	209	69.0%	95.7%
United States	13	4.3%	100.0%
Company			
Communication	15	5.0%	5.0%
Consumer Goods	54	17.8%	22.8%
Durable Goods	2	0.7%	23.4%
Energy	3	1.0%	24.4%
Finance	24	7.9%	32.3%
Government	23	7.6%	39.9%
Healthcare	36	11.9%	51.8%
Hospitality	10	3.3%	55.1%
IT	34	11.2%	66.3%
Industry	36	11.9%	78.2%
Materials	5	1.7%	79.9%
Other	12	4.0%	83.8%
Real Estate	2	0.7%	84.5%
Research and Education	44	14.5%	99.0%
Utilities	3	1.0%	100.0%
Job			
Apprentice	1	0.3%	0.3%
Division Manager/ Managing Director	11	3.6%	4.0%
Employee	162	53.5%	57.4%
Group-/ Teamleader	75	24.8%	82.2%
Head of Department/ Subdivision	45	14.9%	97.0%
Other	1	0.3%	97.4%
Temporary Help	1	0.3%	97.7%
Trainee	1	0.3%	98.0%
Working Student	6	2.0%	100.0%

Table 6 Reliability and validity measurements. CA=Cronbach's alpha, RA=rho_A, CR=composite reliability, AVE=average variance extracted

Construct	CA	RA	CR	AVE
AI identity	0.946	0.948	0.944	0.681
AI identity threat	0.956	0.958	0.955	0.640
Age	1.000	1.000	1.000	1.000
Loss of autonomy	0.933	0.936	0.933	0.823
Changes to work	0.936	0.939	0.934	0.742
Loss of controllability	0.904	0.924	0.907	0.768
Country	1.000	1.000	1.000	1.000
Gender	1.000	1.000	1.000	1.000
Loss of skills/expertise	0.900	0.918	0.902	0.701
Loss of status position	0.936	0.940	0.936	0.711
Threat to job security	0.901	0.905	0.901	0.753

with results higher than 0.50, i.e., a minimum of 50 percent of the variance of the construct's items (Fornell & Larcker, 1981; Hair et al., 2019; Henseler et al., 2016).

The discriminant validity is based on the Fornell-Larcker criterion (Table 10 in the Appendix) (Fornell & Larcker, 1981) and the heterotrait-monotrait (HTMT) ratio (Table 11 in the Appendix) (Henseler et al., 2016). For the Fornell-Larcker criterion, validity can be assumed as the square root of AVE is greater than any inter-factor correlation (Fornell & Larcker, 1981). Regarding HTMT, validity was given to values below 0.90 (Franke & Sarstedt, 2019; Henseler et al., 2016). Harman's one-factor test was conducted, alleviating concerns about common method bias. The variance inflation factors (VIFs) were used to evaluate the collinearity of the formative indicators. The values were below the threshold of 3.30 (Kock, 2015) (Table 12 in the Appendix). We finally observed the cross-loadings excluding incorrect assignment of indicators to constructs (Henseler et al., 2016) (Table 13 in the Appendix).

Structural model analysis

The structural model analysis includes the statistical significance and relevance of the path coefficients, the coefficient of determination, and the blindfolding-based, cross-validated redundancy (Hair et al., 2019). Statistical significance was ascertained by measuring the p values and t statistics (Greenland et al., 2016), where $p \leq 0.05$ and $t > 1.96$ values are sufficient. Cohen's f^2 was calculated to explain statistical relevance. Weak, medium, or large effect sizes ranged from 0.02 to 0.15, 0.15 to 0.35, or greater than or equal to 0.35 (Benitez et al., 2020). R^2 demonstrates explanatory power (Shmueli & Koppius, 2011) with values between 0 and 1: 0.25 is considered weak, 0.5 is moderate, and 0.75 or above is substantial (Hair et al., 2011; Reinartz et al., 2009).

To support explanatory significance, we calculated the Stone-Geisser measure Q^2 to determine predictive relevance, i.e., explaining how well the data can be reproduced by the research model (Geisser, 1974; Stone, 1974). Satisfying results were above 0; values higher than 0, 0.25, and 0.5 were considered small, medium, and large effect sizes (Hair et al., 2019). The goodness of fit as a global validation index for the efficiency of a model (Henseler & Sarstedt, 2013; Tenenhaus et al., 2005) was assessed using AVE and R^2 (adjusted). This resulted in 0.66, which is above the threshold of 0.36, indicating a valid research model (Wetzels et al., 2009). We controlled our model using the participants' ages, genders, and countries, which we found to be insignificant (Table 7).

Finally, we validated the moderating role of AI identity on the effects of threat source factors (e.g., loss of autonomy, changes at work, loss of controllability, loss of skills/expertise, loss of status position and threat to job security) on AI identity threat. However, there were no significant correlations (p values between 0.21 and 0.78).

Table 7 Major effects measurements. O=original sample, M=sample mean, SD=standard deviation, t=t statistic, p=p value

Path	O	M	SD	t	p
AI identity → AI identity threat	-0.175	-0.175	0.059	2.977	0.003
Age → AI identity threat	-0.058	-0.057	0.050	1.156	0.248
Loss of autonomy → AI identity threat	-0.038	-0.033	0.069	0.546	0.585
Changes to work → AI identity threat	0.197	0.199	0.050	3.920	0.000
Loss of controllability → AI identity threat	-0.094	-0.101	0.057	1.651	0.099
Country → AI identity threat	-0.004	-0.003	0.045	0.095	0.924
Gender → AI identity threat	-0.011	-0.012	0.043	0.252	0.801
Loss of skills/expertise → AI identity threat	0.033	0.027	0.103	0.320	0.749
Loss of status position → AI identity threat	0.550	0.561	0.125	4.404	0.000
Threat to job security → AI identity threat	0.112	0.109	0.081	1.391	0.164

Multi-group analysis

Group differences were calculated using the partial least squares multi-group analysis (PLS-MGA) and statistically tested (Reinartz et al., 2009) against the null hypothesis of no significant variations between the groups. Significant differences of path coefficients were indicated by *p* values below 0.05 or above 0.95 (Reinartz et al., 2009). We validated three group differences: employees who work with AI in their companies (*N* = 143; 47.3%) compared to individuals who do not use this technology (*N* = 159, 65.7%), participants who have been using AI in the workplace for a short time (less than 2 years) (*N* = 87; 54.7%), and those who are familiar with handling a system (more than 2 years of experience) (*N* = 64; 45.3%). All hypotheses (H1a,b; H2a,b; H3a,b; H4) were evaluated for each group separately and tested for significant differences between the groups in their parameter estimates. The results indicate that the same set of hypotheses were significant in each subgroup and that there were no existing differences.

Qualitative evaluation

Initially, the experts elaborated on the uniqueness of AI within IT (see Table 14 in the appendix). Overall, the interviewees agreed that AI differs in specific aspects from IT. As E2 explained, “AI and IT are not substituting but complementary to each other.” E5 emphasized that the development of AI is based on algorithms and methods that are also found in IT. However, all experts agreed that AI exceeds the limits of IT by providing functionalities for analyzing data that is IT not capable of. For example, E3 mentioned that AI could lead to the creation of a “blackbox”. Humans may impact the results by manipulating parameters, but, unlike with IT, the employee loses full control of the procedure. E6 supported this perspective, explaining that individuals “cannot determine how the algorithm makes decisions. This is how AI differs from IT.” From a managerial perspective, E6 emphasized that “IT does not reduce headcounts—AI does.” Furthermore, E6 postulated that “AI and IT have to co-exist” but “IT computes the data as it is...AI is able [to get] insights from the data itself.” Based on the feedback of the experts, it can be argued that AI and IT might have the same origin, but AI provides functionalities that break the limits of IT. AI further entails challenges such as replacing human tasks or black-boxing the process of decision-making. These aspects may evoke a unique perception of employees toward AI compared to IT.

To evaluate the identified predictors, we presented the research model to the interviewees. To avoid bias regarding the statistical signifiers, the empirical results were initially disclosed. The experts agreed that the derived research model was comprehensive. The interviewees did

not disagree with a single identified predictor, and E3 concluded that “no predictor seems extraneous or missing.” Thus, all predictors are perceived as important and crucial in the context of AI identity threat. We next asked the experts which predictors could be of particular relevance when the experts mentioned changes to work (E1, E5), job security (E1, E2, E5), loss of status position (E1), loss of skills/expertise (E2, E3), loss of controllability (E2, E3, E4, E5), loss of autonomy (E4, E6), and AI identity (E6) as the most important. All the experts agreed that the workplace changes when introducing AI, and E1 and E5 particularly highlighted the predictors of changes to work as a relevant influence on AI identity threat. Both perceived this as closely linked to the job. When introducing AI in the workplace, the experts emphasized the need for briefing the employees about the function, role, and capabilities of the specific AI. If this step is not done properly, threats related to job security and changes to work increase. Furthermore, E2 mentioned that the degree of perceived threat may differ between the levels of hierarchies: “There are employees who are still 1-2 hops away from being directly affected by AI. The focus is on indirectness that simple jobs are indirectly eliminated by AI. Here, a distinction must be made between management and positions such as mechanics.”

E1 highlighted that introducing AI might not only affect the perception of changes of work and job security but also significantly impacts perceived status positions in the workplace. E1 described this issue as follows: “It is sometimes unclear how good a person is at the job. However, AI requires a process to be measurable. As a result, it then becomes apparent that the human is not good at his job.” Furthermore, E1 distinguished between employee and manager perspectives. From an employee perspective, the human loses; from a managerial perspective, the company wins.

Considering the predictor loss of skills/expertise, E2 mentioned that a possible loss of skills may increase over time, thus potentially turning into a major threat. In contrast, E1 argued that there are use cases in which AI functions as a “preserver of knowledge.” However, E3 emphasized focusing on the human rather than the technology. Thus, AI might provide certain knowledge, but individual employees might lose abilities in the long run. E4 supported this argument by elaborating that “AI could provide knowledge and skills”; thus, the employee is not required to maintain knowledge.

Expertise with AI is also closely related to feelings of losing autonomy and controllability (E2). As AI is capable of performing certain tasks, this may lead to situations in which humans are not able to control certain conditions (E2, E3). Thus, working with AI also involves employees providing data regarding their own actions and work. E4 mentioned that “once the data is out there, the employee has no control over the data.” Likewise, E3 described that a loss of autonomy in the workplace indicates loss of controllability, as “if

I am no longer autonomous, I lose a controllable environment. These factors are interrelated, they merge.” Regarding the feedback from E6, AI identity is one crucial factor that should be considered when broadening our understanding of AI identity threat: “human experience is very important, and decisions should not be accepted without supervision.” The employee should remain the central element in the workplace, and perceptions of and experiences with AI are fundamental for the process of introducing it to the workplace (E6).

The experts also provided valuable insights on strategies countering the AI identity threat by considering the identified predictors. One major factor that was mentioned is the human itself. For “shaping a better tomorrow” (E4) and reducing the negative impact of AI on humans, organizations need trustworthy, ethical, and responsible employees (E4, E6, E5). Currently, “AI is trained by humans with agenda and motivation” (E4). The output provided by AI is based on (input) data that sometimes lacks context; thus, a responsible employee needs to supervise the decision-making process (E6). However, employees need insights into the AI’s black box to understand its results. Thus, explainable AI is needed to better understand the underlying processes (E2, E3, E5, E6).

Discussion

With the ongoing excitement of AI in electronic markets, human-AI interaction is increasingly being accepted by society, transforming enterprises across the globe (Adam et al., 2020; Guan et al., 2020; Thiebes et al., 2020). Organizations strive to understand the impact of AI on humans (Neuhofer et al., 2020), especially how AI can be introduced in the workplace to interact with employees. However, along with benefits for organizations, novel negative consequences for individuals arise. It is thus crucial to comprehend related drawbacks to reduce or eliminate the impacts of the dark sides of AI.

In this study, we identified predictors contributing to AI identity threat in the workplace, such as employees’ perception of AI as indispensable (Mirbabaie et al., 2020). To this end, the evaluated research model explains 56% of the variance of AI identity threat in the workplace. Three out of our seven constructs in the model are substantial, confirming hypotheses H1b, H2b, and H4. Therefore, we answer our research question by identifying loss of status position, changes to work, and AI identity as significant predictors influencing AI identity threat to employees with AI experience in the workplace. These findings are in accordance with the evaluation of the interviewed experts, who fully supported the derived research model.

First, the construct of loss of status position positively impacts AI identity threat. This is in line with the findings of Jussupow et al. (2018), who found that AI acts as a direct threat to the social position of an employee. Therefore, employees who fear a loss of their own competences or independence by AI tend to perceive a higher AI identity threat. For example, we asked the participants about their perception of statements such as “The introduction of AI will reduce my competences” or “By the introduction of AI, I am limited in my possibilities.” In accordance, Israeli (2019) described that employees seek to be perceived as accountable for their work and to enjoy their colleagues’ and clients’ appreciation. By introducing AI in a collaborative setting, employees might expect a loss of their competence and possibilities that lead to a threat to one’s identity. Thus, we are contributing to the threat source of intergroup conflict, by identifying the construct loss of status position as a relevant AI identity threat predictor (Craig et al., 2019). Identity threats classified in the domain of intergroup conflicts are, for example, connected to the reputation and self-beliefs within a team at work. Thus, the construct of loss of status position mirrors the impact on AI identity threat on a professional identity level (Jussupow et al., 2018). Understanding this relationship might be crucial for reducing harmful effects of AI on the employees.

Second, the construct of changes to work according to the threat source category verification prevented positively affects AI identity threat of employees in the workplace. This is in accordance with Craig et al. (2019), who report that introducing a new technology is often related to changes in the workplace. This becomes particularly evident from the results of the interviews, which emphasized the unique possibilities of AI in relation to IT. Thus, the findings suggest that, for example, employees who perceive more responsibilities but also the increased importance of their job positions tend to observe higher identity threat caused by AI. This could be due to the assumption that employees do not feel sufficiently prepared for the introduction of AI (Grundner & Neuhofer, 2021). These harmful influences on the identity of employees are based on personal perception and inspection of self-beliefs initiated or influenced by technology (Craig et al., 2019). In this context, employees need to reevaluate their traditional roles and responsibilities in light of upcoming changes in their workplaces (Craig et al., 2019; Hicks, 2014). This reevaluation takes place on the level of professional identity (Brooks et al., 2011; Jussupow et al., 2018).

Considering these two key findings reveals that the perceived change of work as well as the perceived loss of status position leads to higher AI identity threat. Subsequently, employees may perceive a loss of self-esteem in the domains of worth, competence, and authenticity (Craig et al., 2019).

As a third key finding, this study identified the construct of AI identity as a negative predictor for AI identity threat.

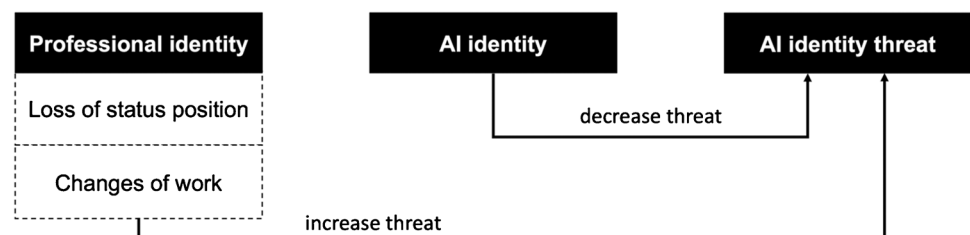
However, the findings did not show a moderating effect of AI identity on the identified predictors of the AI identity threat (e.g., loss of status position, changes of work, or loss of autonomy). Thus, we can assume that AI identity is an independent predictor for further understanding and reducing the identity threat caused by AI. Nevertheless, the identification with AI does not directly impact the specific threat sources evoked by AI itself. From this we can conclude that employees who perceive interaction with AI as an indispensable component of their work perceive lower threat of AI to their identities. This in line with Craig and colleagues (Craig et al., 2019) describing the basic premise of the identity threat caused by technology as the anticipation of further harm leading to resistance behavior in the workplace. A positive association with AI could reduce resistance behavior and support the individual acceptance of AI. This supports the assumptions that humans and technology complement each other when individuals form their identities with technology as an integral component of themselves (Park & Kaye, 2019). Mirbabaie et al. (2021) reveal a connection between identification with AI as a teammate as well as a significant part of the employee's identity. After forming this intertwinement (Carter and Grover, 2015), users tend to be more committed to working with AI conforming to their identities (Deci & Ryan, 2012; Reyshav et al., 2019). A positive AI identity might stabilize individuals' self-esteem related to AI and therefore reduce anticipated identity threats caused by AI (Carter and Grover, 2015; Craig et al., 2019; Petriglieri, 2011). Furthermore, establishing a positive AI identity in the workplace may strengthen one's professional identity by reducing the harmful influence of the identity threat caused by AI. This interplay of the levels of identity, professional identity, and AI identity might be related to a positive development of self-identity (Carter and Grover, 2015; Craig et al., 2019; Park & Kaye, 2019). To better conceptualize the findings of this study, Figure 4 introduces the aggregated formation of predicting AI identity threat in the workplace.

In contrast, this study identified further possible predictors of the AI identity threat in the workplace that did not show significance but were highlighted by the experts. Within meaning change, autonomy illustrates the independent behavior of employees in the workplace, and

controllability refers to the perceived control of employees. Recent research has identified these factors as major threats to identity (Bernardi & Exworthy, 2020; Craig et al., 2019) and extensions of professional identity in the workplace, further related to personal skills and efforts (Jussupov et al., 2018). However, the findings in this study did not provide significance. Thus, employees' perception of losing of skills, autonomy, controllability, or their jobs as a result of the introduction of AI does not seem to influence a possible threat to AI identity in the context of AI-experienced employees. We interpret this to the mean that these constructs might be relevant when introducing AI in the workplace but are not relevant to this study's focus (Carter and Grover, 2015; Craig et al., 2019). As literature as well as the qualitative findings hint at an essential role, we assume that the predictors are valid considering a different sample with divergent characteristics (i.e., no AI experience or expertise). In contrast to the findings of Mirbabaie et al. (2020), who describe a symbiotic association of identification with AI and colleagues, this study reveals how the predictors allocated to professional identity impact the identities of employees when introducing AI in the workplace. Looking closer at the construct of AI identity reveals that the initial measurement item of dependence was removed during the examination of indicator loadings to achieve a first-order construct with significant reliability (Fornell & Larcker, 1981; Hair et al., 2011, 2019). This needs to be mentioned in the context of the study by Carter (2012), from which the items were adapted, analyzed, and conceptualized referring to smartphones. We comprehend that AI, on the one hand, is not really a haptic object comparable to smartphones and, on the other, is currently not very widespread. It thus seems that dependence might not be a decisive factor (yet). AI is somewhat perceived as a component "floating around", which clearly distinguishes it from traditional IT and explains why the original scale does not fit precisely.

Furthermore, the findings of this study do not support that a specific degree of experience with AI in the workplace alters the impact of the identified predictors. This contradicts the assumption that employees might not know what AI is really capable of and have a restricted perception of what collaboration with AI at their workplace would mean for them (Johnson & Verdicchio, 2017; Kühl et al., 2019). Thus, the attitude towards AI in

Fig. 4 Aggregated formation of predictors for AI identity threat in the workplace



the workplace might be detached from individual AI experience and anchored at a common AI setting.

This research is not free of limitations. The theoretical character of the identification of the predictors could be a limiting factor. Asking employees about potential influences may deliver further predictors that this study did not consider. In this context, two out of four items of the scale of loss of skills/expertise refer to the individual perception of employees in general that might influence the relationship with AI identity threat. However, this study is based on an extensive SLR that covers several studies, including qualitative and quantitative research. Therefore, knowledge about IT and AI identity threat is accumulated in this work. AI is a fast-developing technology that will impact the workplace over the coming decades. We thus suggest future research that evaluates predictors of AI identity threat. As this study is based on a sample with AI experience, we suggest that further research should focus on employees without AI experience. Additionally, we suggest that further research should consider the identified constructs when investigating human-AI collaboration in the workplace. As this research is in the IS discipline, the findings are mostly based in this research domain. As IS research is interdisciplinary, this study already covers insights from various scientific perspectives. However, further predictors might be revealed by extending this study to research fields that are not connected or are only minorly connected to the IS community.

Conclusion

In this research, we focused on AI identity threat, which is constructed by employees facing potential collaboration with AI. This study proposes a theoretical framework that identifies predictors of AI identity threat. Overall, our developed research model explains 56% of the variance of AI identity threat in the workplace. We found that changes to work, loss of status position, and AI identity are significant predictors. Furthermore, we indicated that experience with AI does not alter the perception of AI identity threat.

This study contributes to identity research by elaborating the role of AI as a unique technology in the context of identity threat in the workplace. Furthermore, this study reveals the urgent need for research focusing on the impact of AI on the individual. To this end, this study introduces and defines the concepts of the AI identity threat and AI identity by conducting an SLR and expert interviews. This study broadens the understanding of the identity threat caused by AI by revealing loss of status position, changes of work, and AI identity as significant predictors for resolving

Table 8 Experts Characteristics

Expert	Age	Gender	Job Position
E1	38	Male	Manager data science
E2	33	Male	Technical management
E3	37	Male	Department manager
E4	38	Male	Senior data scientist
E5	32	Male	Analyst IT consulting
E6	24	Male	Change management consultant

the AI identity threat in the workplace. To this end, this study develops a research model to broaden our understanding of the AI identity threat. Regarding the identity theory's threat sources, loss of status position could be assigned to the domain of intergroup conflict and changes of work to verification prevented. This allocation gains importance when developing counteractions for reducing the AI identity threat. In summary, we reveal fundamental factors related to the negative impacts of AI on humans, the so-called dark side of AI.

This study further contributes to practice by revealing specific influencing factors that should be considered when introducing AI in the workplace. Practitioners may consider that individual experience with AI seems less relevant than expected by the literature. However, by first explaining and defining AI identity and further revealing influencing factors on employees' identities in the workplace, practitioners should consider the special role of identity in the context of human-AI collaboration. Decision makers, such as managers and executives, may consider these insights to reduce upcoming resistance to AI in the workplace. Furthermore, it is vital to support a positive identification with AI in the workplace to reduce potential threats to employees' identities. This might be achieved by reducing potential threats evoked by expected changes to work or personal status position. Based on the experts' evaluation, we further suggest introducing explainable AI as well focusing on trustworthy, responsible, and ethical employees who supervise AI implementations and applications.

In terms of contributions to society, this study suggests a symbiotic relationship between humans and AI to support human self-esteem and well-being in the workplace. Through continuing education about AI's capabilities in electronic markets, individuals and enterprises may use AI as a technology to extend their skills and competences in the workplace.

Appendix

Table 9 Measurement items

No	Item
AI identity (M = 3.75; SD = 1.30; α = 0.946; adapted from Carter (2012))	
AID001	Thinking about myself in relation to AI, I feel enthusiastic
AID002	Thinking about myself in relation to AI, I feel pumped up
AID003	Thinking about myself in relation to AI, I feel energized
AID004	Thinking about myself in relation to AI, I feel confident
AID005	Thinking about myself in relation to AI, I am close to AI
AID006	Thinking about myself in relation to AI, I am connected with AI
AID007	Thinking about myself in relation to AI, I am in coordination to AI
AID008	Thinking about myself in relation to AI, I am linked with AI
AI identity threat (M = 2.41; SD = 1.17; α = 0.957; adapted from Craig et al. (2019))	
AIT001	If I use AI with enthusiasm, people in my peer group will lose respect for me
AIT002	If I seem to support AI, I will feel that others will consider me to be a poor member of my peer group
AIT003	Embracing AI makes me feel less respected by others in my peer group
AIT004	Using AI with enthusiasm makes me feel that people in my peer group will admire me less
AIT005	Using AI makes me feel less confident that I understand things well enough to get work done
AIT006	Using AI makes me feel that I have less ability to get work done
AIT007	Using AI makes me feel less confident about having the skills and knowledge needed to get work done
AIT008	Using AI makes me feel that I do things poorly
AIT009	Using AI makes me feel discouraged with who I am
AIT010	Using AI makes me feel displeased with who I am
AIT011	Using AI makes me feel less like the person I want to be
AIT012	Using AI makes me feel that I have fewer of the qualities that make me stand out as a person
Loss of autonomy (M = 5.15; SD = 1.22; α = 0.933; adapted from Breugh (1985))	
AUT001	I am allowed to decide how to go about getting my job done (the methods to use)
AUT002	I am able to choose the way to go about my job (the procedures to utilize)
AUT003	I am free to choose the method(s) to use in carrying out my work
Changes of work (M = 3.49; SD = 1.36; α = 0.938; self-developed, validated in pre-study)	
CHW001	The introduction of AI increases my area of responsibility
CHW002	The introduction of AI makes my job more important than before
CHW003	Since the introduction of AI, I am responsible for more things
CHW004	By the introduction of AI, I am responsible for more tasks
CHW005	Since the introduction of AI, my organization expects me to take on more responsibility
Loss of controllability (M = 5.01; SD = 1.34; α = 0.903; adapted from Breugh (1985))	
CON001	I have control over the scheduling of my work
CON002	I have some control over sequencing of my work activities (when I do what)
CON003	My job is such that I can decide when to do particular work activities
Loss of skills/expertise (M = 3.52; SD = 1.49; α = 0.901; adapted from Jussupow et al. (2018))	
LSE001	I fear that when using AI, employees may lose their expert status
LSE002	I fear that when using AI, specialized work-related skills will not be needed anymore

Table 9 (continued)

No	Item
LSE003	I fear that when using AI, certain specializations can be replaced
LSE004	I fear that when using AI, employees may feel less competent
Loss of status position (M = 2.99; SD = 1.39; α = 0.937; self-developed, validated in pre-study)	
LSP001	The introduction of a AI will reduce my competences
LSP002	I think that my position will be less important with the introduction of AI
LSP003	I think that after the introduction of AI, I can no longer decide everything on my own
LSP004	After the introduction of AI, in the future only the system decides
LSP005	By the introduction of AI, I am limited in my possibilities
LSP006	With the introduction of AI, I no longer have as much to say as before
Threat to job security (M = 2.77; SD = 1.57; α = 0.901; adapted from Hellgren et al. (1999))	
TJS001	I am worried about having to leave my job before I would like to
TJS002	There is a risk that I will have to leave my present job in the year to come
TJS003	I feel uneasy about losing my job in the near future

Table 10 Fornell-Larcker Criterion, (1) AI identity, (2) AI identity threat, (3) age, (4) loss of autonomy, (5) changes of work, (6) loss of controllability, (7) country, (8) gender, (9) loss of skills/expertise, (10) loss of status position, (11) threat to job security

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)
(1)	0.826										
(2)	-0.247	0.800									
(3)	-0.130	-0.008	1.000								
(4)	0.223	-0.390	0.054	0.907							
(5)	0.462	0.049	-0.054	0.092	0.861						
(6)	0.206	-0.249	0.050	0.537	0.195	0.877					
(7)	0.029	0.014	0.238	0.069	0.021	0.058	1.000				
(8)	-0.081	0.027	0.020	0.078	-0.043	0.033	0.207	1.000			
(9)	-0.209	0.606	0.070	-0.370	-0.042	-0.184	0.077	0.097	0.837		
(10)	-0.238	0.710	0.080	-0.406	-0.077	-0.189	0.065	0.055	0.809	0.843	
(11)	-0.048	0.550	-0.005	-0.363	-0.046	-0.207	0.046	0.063	0.654	0.698	0.868

Table 11 HTMT, (1) AI identity, (2) AI identity threat, (3) age, (4) loss of autonomy, (5) changes of work, (6) loss of controllability, (7) country, (8) gender, (9) loss of skills/expertise, (10) loss of status position, (11) threat to job security

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)
(1)	-										
(2)	0.238	-									
(3)	0.127	0.038	-								
(4)	0.219	0.388	0.054	-							
(5)	0.460	0.079	0.058	0.093	-						
(6)	0.210	0.245	0.055	0.534	0.196	-					
(7)	0.039	0.028	0.238	0.069	0.030	0.060	-				
(8)	0.082	0.044	0.020	0.078	0.042	0.032	0.207	-			
(9)	0.199	0.591	0.072	0.375	0.048	0.178	0.091	0.093	-		
(10)	0.228	0.703	0.081	0.403	0.081	0.182	0.067	0.054	0.809	-	
(11)	0.120	0.545	0.011	0.363	0.047	0.206	0.044	0.063	0.657	0.698	-

Table 12 Inner variance inflations

Construct	AI identity threat
AI identity	1.470
AI identity threat	-
Age	1.099
Loss of autonomy	1.693
Changes of work	1.312
Loss of controllability	1.463
Country	1.123
Gender	1.080
Loss of skills/expertise	3.100
Loss of status position	3.290
Threat to job security	2.190

Table 13 Cross-loadings, (1) AI identity, (2) AI identity threat, (3) age, (4) loss of autonomy, (5) changes of work, (6) loss of controllability, (7) country, (8) gender, (9) loss of skills/expertise, (10) loss of status position, (11) threat to job security

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)
(1) [AID001]	0.925	-0.378	-0.097	0.234	0.376	0.200	0.077	-0.074	-0.313	-0.360	-0.205
(1) [AID002]	0.835	-0.178	-0.176	0.163	0.384	0.156	-0.010	-0.057	-0.206	-0.192	-0.023
(1) [AID003]	0.906	-0.198	-0.200	0.227	0.422	0.178	0.002	-0.085	-0.203	-0.223	-0.078
(1) [AID004]	0.849	-0.381	-0.087	0.287	0.328	0.236	0.061	-0.041	-0.281	-0.327	-0.217
(1) [AID005]	0.799	-0.080	-0.082	0.136	0.427	0.186	0.002	-0.071	-0.101	-0.083	0.065
(1) [AID006]	0.677	-0.109	-0.065	0.121	0.328	0.147	0.063	-0.098	-0.062	-0.094	0.048
(1) [AID007]	0.783	-0.126	-0.044	0.151	0.393	0.131	0.020	-0.078	-0.082	-0.112	0.068
(1) [AID008]	0.804	-0.137	-0.089	0.132	0.397	0.120	-0.023	-0.040	-0.087	-0.135	0.082
(2) [AIT001]	-0.190	0.843	0.002	-0.263	0.057	-0.207	0.033	0.006	0.514	0.617	0.440
(2) [AIT001]	-0.190	0.798	-0.028	-0.237	0.063	-0.165	-0.005	-0.021	0.506	0.572	0.455
(2) [AIT001]	-0.179	0.770	0.044	-0.222	0.049	-0.160	0.020	0.028	0.502	0.560	0.438
(2) [AIT001]	-0.197	0.815	-0.043	-0.291	0.035	-0.199	0.005	0.024	0.524	0.579	0.438
(2) [AIT001]	-0.243	0.837	0.014	-0.321	-0.015	-0.185	0.048	0.112	0.521	0.595	0.457
(2) [AIT001]	-0.245	0.979	-0.017	-0.393	-0.018	-0.239	0.042	0.063	0.605	0.701	0.555
(2) [AIT001]	-0.166	0.848	-0.049	-0.365	0.023	-0.208	0.041	0.017	0.573	0.606	0.475
(2) [AIT001]	-0.222	0.830	-0.073	-0.364	-0.002	-0.186	-0.003	0.063	0.543	0.579	0.432
(2) [AIT001]	-0.180	0.677	0.006	-0.312	0.067	-0.170	-0.039	-0.034	0.332	0.474	0.383
(2) [AIT001]	-0.176	0.722	0.011	-0.362	0.094	-0.224	-0.009	0.014	0.374	0.493	0.405
(2) [AIT001]	-0.188	0.720	0.055	-0.303	0.095	-0.203	-0.003	-0.007	0.386	0.500	0.391
(2) [AIT001]	-0.188	0.715	0.021	-0.305	0.059	-0.247	-0.021	-0.034	0.372	0.495	0.385
(3) [AGE]	-0.130	-0.008	1.000	0.054	-0.054	0.050	0.238	0.020	0.070	0.080	-0.005
(4) [AUT001]	0.177	-0.337	0.061	0.859	0.045	0.452	0.038	0.063	-0.340	-0.366	-0.326
(4) [AUT002]	0.222	-0.349	0.041	0.893	0.108	0.477	0.086	0.073	-0.305	-0.349	-0.318
(4) [AUT003]	0.207	-0.373	0.045	0.966	0.096	0.530	0.064	0.077	-0.360	-0.389	-0.343
(5) [CHW001]	0.403	0.021	-0.110	0.109	0.897	0.189	0.049	-0.025	-0.039	-0.046	-0.044
(5) [CHW002]	0.425	-0.033	-0.043	0.158	0.949	0.200	-0.018	-0.077	-0.075	-0.104	-0.091
(5) [CHW003]	0.396	0.061	-0.072	0.058	0.855	0.158	0.002	-0.026	-0.018	-0.071	-0.031
(5) [CHW004]	0.409	0.073	0.012	0.028	0.846	0.148	0.045	-0.022	-0.022	-0.066	-0.027
(5) [CHW005]	0.353	0.108	-0.014	0.029	0.747	0.137	0.014	-0.033	-0.020	-0.039	0.005
(6) [CON001]	0.217	-0.146	0.089	0.370	0.183	0.730	0.054	0.024	-0.113	-0.116	-0.136
(6) [CON002]	0.175	-0.266	0.022	0.542	0.168	0.988	0.040	0.050	-0.171	-0.193	-0.218
(6) [CON003]	0.161	-0.229	0.032	0.485	0.166	0.893	0.062	0.009	-0.193	-0.179	-0.183
(7) [COU]	0.029	0.014	0.238	0.069	0.021	0.058	1.000	0.207	0.077	0.065	0.046
(8) [GEN]	-0.081	0.027	0.020	0.078	-0.043	0.033	0.207	1.000	0.097	0.055	0.063
(9) [LSE001]	-0.180	0.590	0.049	-0.328	-0.032	-0.203	0.090	0.089	0.929	0.737	0.591
(9) [LSE002]	-0.216	0.559	0.087	-0.304	-0.066	-0.163	0.078	0.119	0.922	0.758	0.584
(9) [LSE003]	-0.093	0.341	0.082	-0.310	-0.030	-0.075	-0.035	0.015	0.641	0.543	0.477
(9) [LSE004]	-0.194	0.506	0.021	-0.306	-0.007	-0.155	0.101	0.085	0.823	0.652	0.534
(10) [LSP001]	-0.153	0.534	0.077	-0.249	0.019	-0.102	0.084	0.005	0.603	0.733	0.539
(10) [LSP002]	-0.167	0.628	0.040	-0.383	-0.052	-0.212	0.034	0.006	0.692	0.893	0.671
(10) [LSP003]	-0.147	0.526	0.071	-0.308	-0.023	-0.057	0.058	0.051	0.655	0.765	0.549
(10) [LSP004]	-0.206	0.623	0.076	-0.335	-0.066	-0.176	0.044	0.098	0.690	0.847	0.558
(10) [LSP005]	-0.277	0.634	0.045	-0.422	-0.120	-0.248	0.028	0.060	0.728	0.932	0.646
(10) [LSP006]	-0.240	0.636	0.103	-0.338	-0.127	-0.134	0.089	0.053	0.722	0.872	0.562
(11) [TJS001]	-0.069	0.526	-0.017	-0.328	-0.050	-0.185	0.078	0.064	0.603	0.654	0.935
(11) [TJS002]	-0.026	0.445	-0.004	-0.309	-0.039	-0.169	0.013	0.075	0.535	0.564	0.815
(11) [TJS003]	-0.025	0.458	0.009	-0.308	-0.030	-0.186	0.023	0.026	0.563	0.597	0.849

Table 14 Procedure and guiding questions of the semi-structured expert interviews

Step	Area	Question / Comment
1	Introduction	<i>The goal of this study is to take a closer look at the "Dark Side of AI." To this end, we look at the extent to which artificial intelligence as a technology influences our identity and what consequences arise from the introduction and use of AI in the workplace. To this end, we have analyzed existing literature and identified influencing factors that can affect harm caused by AI. We now want to evaluate these</i>
2	Demographics	What is your current position in your company?
3		How long have you been working in your company?
4		What is the core business of your company?
5		To which industry would you classify your company?
6	Artificial Intelligence	What do you associate with the term "Artificial Intelligence"?
7		What experience have you already had with AI? / What have you already used AI for?
8		Definition of AI that can be provided: <i>"The ability of a machine to perform cognitive functions that we associate with the human mind, such as perception, reasoning, learning, interacting with the environment, problem solving, decision making, and even demonstrating creativity."</i>
		Examples of AI in enterprises that can be provided: <i>Process support, replacement for repetitive tasks, Virtual Assistants to help with tasks</i>
9		How does AI differ from IT?
10		What makes AI unique in this context?
11	What are the commonalities between AI and IT?	
12	Evaluation of the research model / identified predictors	Have subjects look at the model
		Definition of IT/AI Identity that can be provided: <i>The extent to which a person considers the use/collaboration of an IT/AI to be an integral part of their self-image</i>
		Definition of IT-Identity Threat that can be provided: <i>The expectation of harm to an individual's identity/self-awareness caused by the use of an IT. The "target" of the harm is the individual user of an IT</i>
13		How do you evaluate the model?
14		How do you evaluate the identified predictors?
15		What other factors can you think of that the model does not take into account?
16	In your opinion, what is the most important aspect to consider when introducing AI in the workplace (to avoid negative influences of AI on employees)?	
17	Conclusion	Are there any other questions you would have expected in connection with ours, but which we have not asked?
		Would you like to add further aspects to the topic?

Funding Open Access funding enabled and organized by Projekt DEAL.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

- About, F. (2020). The effect of E: Learning on EFL teacher identity. *International Journal of English Research*, 6(2), 22–27.
- Abouzahra, M., Guenter, D., & Tan, J. (2015). Integrating Information Systems and Healthcare Research to Understand Physicians' use of Health Information Systems: a Literature Review. *36th International Conference on Information Systems*. Presented at the International Conference on Information Systems, Fort Worth
- Acemoglu, D., & Restrepo, P. (2018). The Race between Man and Machine: Implications of Technology for Growth, Factor Shares, and Employment. *American Economic Review*, 108(6), 1488–1542. <https://doi.org/10.1257/aer.20160696>
- Adam, M., Wessel, M., & Benlian, A. (2021). AI-based chatbots in customer service and their effects on user compliance. *Electronic Markets*, 31(2). <https://doi.org/10.1007/s12525-020-00414-7>
- Alahmad, R., & Robert, L. (2020). Artificial Intelligence (AI) and IT identity: Antecedents Identifying with AI Applications. *AMCIS 2020 Proceedings*. (p. 11). Presented at the Americas Conference on Information Systems, Salt Lake City, Utah.
- Aleksander, I. (2017). Partners of Humans: A Realistic Assessment of the Role of Robots in the Foreseeable Future. *Journal of Information Technology*, 32(1), 1–9. <https://doi.org/10.1057/2Fs41265-016-0032-4>

- Ali, H., & Birley, S. (1999). Integrating deductive and inductive approaches in a study of new ventures and customer perceived risk. *Qualitative Market Research: An International Journal*, 2(2), 103–110. <https://doi.org/10.1108/13522759910270016>
- Alt, R. (2018). Electronic Markets and current general research. *Electronic Markets*, 28(2), 123–128. <https://doi.org/10.1007/s12525-018-0299-0>
- Alvarez, R. (2008). Examining technology, structure and identity during an Enterprise System implementation. *Information Systems Journal*, 18(2), 203–224. <https://doi.org/10.1111/j.1365-2575.2007.00286.x>
- Alvesson, M., Lee Ashcraft, K., & Thomas, R. (2008). Identity Matters: Reflections on the Construction of Identity Scholarship in Organization Studies. *Organization*, 15(1), 5–28. <https://doi.org/10.1177/2F1350508407084426>
- Aversa, P., Cabantous, L., & Haefliger, S. (2018). When decision support systems fail: Insights for strategic information systems from Formula 1. *The Journal of Strategic Information Systems*, 27(3), 221–236. <https://doi.org/10.1016/j.jsis.2018.03.002>
- Bandara, W., Furtmueller, E., Gorbacheva, E., Miskon, S., & Beekhuizen, J. (2015). Achieving Rigor in Literature Reviews: Insights from Qualitative Data Analysis and Tool-Support. *Communications of the Association for Information Systems*, 37. <https://doi.org/10.17705/ICAIS.03708>
- Baptista, J., Stein, M.-K., Klein, S., Watson-Manheim, M. B., & Lee, J. (2020). Digital work and organisational transformation: Emergent Digital/Human work configurations in modern organisations. *The Journal of Strategic Information Systems*, 29(2), 101618. <https://doi.org/10.1016/j.jsis.2020.101618>
- Barredo Arrieta, A., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., Garcia, S., Gil-Lopez, S., Molina, D., Benjamins, R., Chatila, R., & Herrera, F. (2020). Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. *Information Fusion*, 58, 82–115. <https://doi.org/10.1016/j.inffus.2019.12.012>
- Batin, M., & Turchin, A. (2017). Artificial Intelligence in Life Extension: From Deep Learning to Superintelligence. *Informatica*, 41, 401–417.
- Bear, A., & Knobe, J. (2017). Normality: Part descriptive, part prescriptive. *Cognition*, 167, 25–37. <https://doi.org/10.1016/j.cognition.2016.10.024>
- Bednar, P. M., & Welch, C. (2020). Socio-Technical Perspectives on Smart Working: Creating Meaningful and Sustainable Systems. *Information Systems Frontiers*, 22(2), 281–298. <https://doi.org/10.1007/s10796-019-09921-1>
- Bell, D. E. (1989). *Decision Making: Descriptive, Normative, and Prescriptive Interactions*. Cambridge University Press.
- Benitez, J., Henseler, J., Castillo, A., & Schuberth, F. (2020). How to perform and report an impactful analysis using partial least squares: Guidelines for confirmatory and explanatory IS research. *Information & Management*, 57(2), 17. <https://doi.org/10.1016/j.im.2019.05.003>
- Bernardi, R., & Exworthy, M. (2020). Clinical managers' identity at the crossroad of multiple institutional logics in it innovation: The case study of a health care organization in England. *Information Systems Journal*, 30(3), 566–595. <https://doi.org/10.1111/isj.12267>
- Boell, S., & Wang, B. (2019). www.litbaskets.io, an IT Artifact Supporting Exploratory Literature Searches for Information Systems Research. *Australasian Conference on Information Systems* (p. 13). Presented at the Australasian Conference on Information Systems, Fremantle, Australia.
- Bogner, A., Littig, B., & Menz, W. (2009). Introduction: Expert interviews — an introduction to a new methodological debate. In A. Bogner, B. Littig, & W. Menz (Eds.), *Interviewing Experts* (pp. 1–13). Palgrave Macmillan UK. https://doi.org/10.1057/9780230244276_1
- Bouckennooghe, D., Devos, G., & Van den Broeck, H. (2009). Organizational Change Questionnaire—Climate of Change, Processes, and Readiness: Development of a New Instrument. *The Journal of Psychology*, 143(6), 559–599. <https://doi.org/10.1080/00223980903218216>
- Boudreau, M.-C., Serrano, C., & Larson, K. (2014). IT-driven identity work: Creating a group identity in a digital environment. *Information and Organization*, 24(1), 1–24. <https://doi.org/10.1016/j.infoandorg.2013.11.001>
- Boudreau, M.-C., Nach, H., & Lejeune, A. M. (2016). Intergroup Collaboration: An Examination through the Lenses of Identity and IT Affordances. *37th International Conference on Information Systems* (p. 10). Presented at the International Conference on Information Systems, Dublin.
- Brachten, F., Brünker, F., Frick, N. R. J., Ross, B., & Stieglitz, S. (2020). On the ability of virtual agents to decrease cognitive load: an experimental study. *Information Systems and e-Business Management*, 18, 187–207. <https://doi.org/10.1007/s10257-020-00471-7>
- Breaugh, J. A. (1985). The Measurement of Work Autonomy. *Human Relations*, 38(6), 551–870. <https://doi.org/10.1177/2F001872678503800604>
- vom Brocke, J., Simons, A., Niehaves, B., Riemer, K., Plaffaut, R., & Clevén, A. (2009). Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process. In: Newell, S., Whitley, E., Pouloudi, N., Wareham, J. & Mathiasen, L. (Eds.), *Proceedings of the ECIS 2009, 17th European Conference On Information Systems, Verona*, 2206–2217.
- Brooks, N. G., Riemenschneider, C. K., Hardgrave, B. C., & O'Leary-Kelly, A. M. (2011). IT professional identity: needs, perceptions, and belonging. *European Journal of Information Systems*, 20(1), 87–102. <https://doi.org/10.1057/ejis.2010.48>
- Burke, P. J., & Stryker, S. (2016). Identity Theory: Progress in Relating the Two Strands. *New Directions in Identity Theory and Research* (pp. 657–810). Oxford University Press.
- Camilleri, J., & Neuhofer, B. (2017). Value co-creation and co-destruction in the Airbnb sharing economy. *International Journal of Contemporary Hospitality Management*, 29(9), 2322–2340. <https://doi.org/10.1108/IJCHM-09-2016-0492>
- Carroll, B., & Levy, L. (2008). Defaulting to Management: Leadership Defined by What It Is Not. *Organization*, 15(1), 75–96. <https://doi.org/10.1177/2F1350508407084486>
- Carter, M. (2012). *Information Technology (IT) Identity: A Conceptualization, Proposed Measures, and Research Agenda*. Clemson University.
- Carter, M., & Grover, V. (2015). Me, My Self, and I(T): Conceptualizing Information Technology Identity and its Implications. *MIS Quarterly*, 39(4), 931–957. <https://doi.org/10.25300/MISQ/2015/39.4.9>
- Carter, M., Petter, S., & Compeau, D. (2019). Identifying with IT in a Digital World. *ICIS 2019 Proceedings* (p. 10). Presented at the International Conference on Information Systems, Munich.
- Carter, M., Petter, S., Grover, V., & Thatcher, J. (2020a). IT Identity: A Measure and Empirical Investigation of its Utility to IS Research. *Journal of the Association for Information Systems*, 21(5), 1313–1342. <https://doi.org/10.17705/1jais.00638>
- Carter, M., Petter, S., Grover, V., & Thatcher, J. B. (2020b). Information Technology Identity: A Key Determinant of IT Feature and Exploratory Usage. *MIS Quarterly*, 44(3), 983–1021. <https://doi.org/10.25300/MISQ/2020/14607>
- Cheng, X., Bao, Y., & Zarifis, A. (2020a). Investigating the impact of IT-mediated information interruption on emotional exhaustion in the workplace. *Information Processing & Management*, 57(6), 1–16. <https://doi.org/10.1016/j.ipm.2020.102281>

- Cheng, X., Sun, J., & Zarifis, A. (2020b). Artificial intelligence and deep learning in educational technology research and practice. *British Journal of Educational Technology*, *51*(5), 1653–1656. <https://doi.org/10.1111/bjet.13018>
- Cheng, X., Su, L., Luo, X. (Robert), Benitez, J., & Cai, S. (2021). 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*, 1–25. <https://doi.org/10.1080/0960085X.2020.1869508>
- Chreim, S., Williams, B. E. (Bernie), & Hinings, C. R. (Bob). (2007). Interlevel Influences on the Reconstruction of Professional Role Identity. *Academy of Management Journal*, *50*(6), 1515–1539. <https://doi.org/10.5465/amj.2007.28226248>
- Churchill, G. A. (1979). A Paradigm for Developing Better Measures of Marketing Constructs. *Journal of Marketing Research*, *16*(1), 64. <https://doi.org/10.2307/3150876>
- Coombs, C., Hislop, D., Taneva, S. K., & Barnard, S. (2020). The strategic impacts of Intelligent Automation for knowledge and service work: An interdisciplinary review. *The Journal of Strategic Information Systems*, *29*(4), 1–30. <https://doi.org/10.1016/j.jsis.2020.101600>
- Cooper, H. M. (1988). Organizing knowledge syntheses: A taxonomy of literature reviews. *Knowledge in Society*, *1*(1), 104–126. <https://doi.org/10.1007/BF03177550>
- Craig, K., Thatcher, J. B., & Grover, V. (2019). The IT Identity Threat: A Conceptual Definition and Operational Measure. *Journal of Management Information Systems*, *36*(1), 259–288. <https://doi.org/10.1080/07421222.2018.1550561>
- Creswell, J. W., & Creswell, D. J. (2018). *Research design: qualitative, quantitative, and mixed methods approaches*. SAGE Publications Ltd.
- D’Mello, M., & Eriksen, T. H. (2010). Software, sports day and sheera. *Information and Organization*, *20*(2), 81–110. <https://doi.org/10.1016/j.infoandorg.2010.03.001>
- da Cunha, J. V., & Orlikowski, W. J. (2008). Performing catharsis: The use of online discussion forums in organizational change. *Information and Organization*, *18*(2), 132–156. <https://doi.org/10.1016/j.infoandorg.2008.02.001>
- Daskalopoulou, A., Palmer, M., Keeling, K., & Pritchard Jones, R. (2019). Discretionary technology bootlegging tensions in institutional healthcare work. *New Technology, Work and Employment*, *34*(1), 73–89. <https://doi.org/10.1111/ntwe.12133>
- Deci, E. L., & Ryan, R. M. (2012). Self-determination theory. In P. A. M. Van Lange, A. W. Kruglanski, & E. T. Higgins (Eds.), *Handbook of theories of social psychology* (pp. 416–436). Sage Publications Ltd. <https://doi.org/10.4135/9781446249215.n21>
- Dellermann, D., Lipusch, N., Ebel, P., & Leimeister, J. M. (2019). Design principles for a hybrid intelligence decision support system for business model validation. *Electronic Markets*, *29*(3), 423–441. <https://doi.org/10.1007/s12525-018-0309-2>
- Diamantopoulos, A., Sarstedt, M., Fuchs, C., Wilczynski, P., & Kaiser, S. (2012). Guidelines for choosing between multi-item and single-item scales for construct measurement: a predictive validity perspective. *Journal of the Academy of Marketing Science*, *40*(3), 434–449. <https://doi.org/10.1007/s11747-011-0300-3>
- Dietvorst, B. J., Simmons, J. P., & Massey, C. (2015). Algorithm Aversion: People Erroneously Avoid Algorithms After Seeing Them Err. *Journal of Experimental Psychology: General*, *144*(1), 114–126. <https://doi.org/10.1037/xge0000033>
- Dijkstra, T. K., & Henseler, J. (2015). Consistent Partial Least Squares Path Modeling. *MIS Quarterly*, *39*(2), 297–316. <https://doi.org/10.25300/MISQ/2015/39.2.02>
- Duan, Y., Edwards, J. S., & Dwivedi, Y. K. (2019). Artificial intelligence for decision making in the era of Big Data – evolution, challenges and research agenda. *International Journal of Information Management*, *48*, 63–71. <https://doi.org/10.1016/j.ijinfomgt.2019.01.021>
- Dwivedi, Y. K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., Duan, Y., Dwivedi, R., Edwards, J., Eirug, A., Galanos, V., Ilavarasan, P. V., Janssen, M., Jones, P., Kumar Kar, A., Kizgin, H., Kronemann, B., Lal, B., Lucini, B., Medaglia, R., Le Meunier-FitzHugh, K., Le Meunier-FitzHugh, L. C., Misra, S., Mogaji, E., KumarSharma, S., Bahadur Singh, J., Raghavan, V., Ramanu, R., P. Rana, N., Samothrakis, S., Spencer, J., Tamilmani, K., Tubadji, A., Walton, P., & Williams, M. D. (2019). Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*, *101994*. <https://doi.org/10.1016/j.ijinfomgt.2019.08.002>
- Elbanna, A., & Linderoth, H. C. J. (2015). The formation of technology mental models: The case of voluntary use of technology in organizational setting. *Information Systems Frontiers*, *17*(1), 95–108. <https://doi.org/10.1007/s10796-014-9513-6>
- Fink, A. (2013). *Conducting Research Literature Reviews: from the Internet to Paper*. Sage Publications, Inc.
- Fornell, C., & Bookstein, F. L. (1982). Two Structural Equation Models: LISREL and PLS Applied to Consumer Exit-Voice Theory. *Journal of Marketing Research*, *19*(4), 440. <https://doi.org/10.2307/3151718>
- Fornell, C., & Larcker, D. F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of Marketing Research*, *18*(1), 39. <https://doi.org/10.2307/3151312>
- Franke, G., & Sarstedt, M. (2019). Heuristics versus statistics in discriminant validity testing: a comparison of four procedures. *Internet Research*, *29*(3), 430–447. <https://doi.org/10.1108/IntR-12-2017-0515>
- Frick, N., & Marx, J. (2021). Integrating Digital Nomads in Corporate Structures: Managerial Contemplations. Presented at the Hawaii International Conference on System Sciences. <https://doi.org/10.24251/HICSS.2021.260>
- Frick, N. R. J., Brünker, F., Ross, B., & Stieglitz, S. (2019). The Utilization of Artificial Intelligence for Improving Incident Management. *HMD Praxis der Wirtschaftsinformatik*, *56*(2), 357–369. <https://doi.org/10.1365/s40702-019-00505-w>
- Frick, N. R. J., Brünker, F., Ross, B., & Stieglitz, S. (2020). Design Requirements for AI-based Services Enriching Legacy Information Systems in Enterprises: A Managerial Perspective. *Proceedings of the 31st Australasian Conference on Information Systems*. Presented at the Australasian Conference on Information Systems, Wellington.
- Frick, N. R. J., Mirbabaie, M., Stieglitz, S., & Salomon, J. (2021). Maneuvering through the stormy seas of digital transformation: the impact of empowering leadership on the AI readiness of enterprises. *Journal of Decision Systems*, 1–24. <https://doi.org/10.1080/12460125.2020.1870065>
- Geertshuis, S., & Liu, Q. (2016). E-learning Ecosystem Awareness and Professional Identity in E-learning Technology Adoption. *15th European Conference on e-learning*. Presented at the European Conference on e-learning.
- Geisser, S. (1974). A Predictive Approach to the Random Effects Model. *Biometrika*, *61*(1), 101–107. <https://doi.org/10.1093/biomet/61.1.101>
- Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2013). Seeking Qualitative Rigor in Inductive Research: Notes on the Gioia Methodology. *Organizational Research Methods*, *16*(1), 15–31. <https://doi.org/10.1177/2F1094428112452151>
- Gong, X., Chen, C., & Lee, M. K. O. (2020). What drives problematic online gaming? The role of IT identity, maladaptive cognitions, and maladaptive emotions. *Computers in Human Behavior*, *110*. <https://doi.org/10.1016/j.chb.2020.106386>

- Goodhue, L., & Thompson, . (2012). Does PLS Have Advantages for Small Sample Size or Non-Normal Data? *MIS Quarterly*, 36(3), 981. <https://doi.org/10.2307/41703490>
- Grant, M. J., & Booth, A. (2009). A typology of reviews: an analysis of 14 review types and associated methodologies: A typology of reviews, *Maria J. Grant & Andrew Booth. Health Information & Libraries Journal*, 26(2), 91–108. <https://doi.org/10.1111/j.1471-1842.2009.00848.x>
- Grønsund, T., & Aanestad, M. (2020). Augmenting the algorithm: Emerging human-in-the-loop work configurations. *The Journal of Strategic Information Systems*, 29(2), 101614. <https://doi.org/10.1016/j.jsis.2020.101614>
- Grundner, L., & Neuhofer, B. (2021). The bright and dark sides of artificial intelligence: A futures perspective on tourist destination experiences. *Journal of Destination Marketing & Management*, 19, 100511. <https://doi.org/10.1016/j.jdmm.2020.100511>
- Guan, C., Mou, J., & Jiang, Z. (2020). Artificial intelligence innovation in education: A twenty-year data-driven historical analysis. *International Journal of Innovation Studies*, 4(4), 134–147. <https://doi.org/10.1016/j.ijis.2020.09.001>
- Haenlein, M., & Kaplan, A. (2019). A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence. *California Management Review*, 61(4), 5–14. <https://doi.org/10.1177/2F0008125619864925>
- Haesevoets, T., De Cremer, D., Dierckx, K., & Van Hiel, A. (2021). Human-machine collaboration in managerial decision making. *Computers in Human Behavior*, 119, 106730. <https://doi.org/10.1016/j.chb.2021.106730>
- Hair, J. F., Hult, G. T. M., Ringle, C. M., Sarstedt, M., & Thiele, K. O. (2017). Mirror, mirror on the wall: A comparative evaluation of composite-based structural equation modeling methods. *Journal of the Academy of Marketing Science*, 45(5), 616–632. <https://doi.org/10.1007/s11747-017-0517-x>
- Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a Silver Bullet. *Journal of Marketing Theory and Practice*, 19(2), 139–152. <https://doi.org/10.2753/MTP1069-6679190202>
- Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS- SEM. *European Business Review*, 31(1), 2–24. <https://doi.org/10.1108/EBR-11-2018-0203>
- You, S., & Robert Jr., L. P. (2018). Emotional Attachment, Performance, and Viability in Teams Collaborating with Embodied Physical Action (EPA) Robots. *Journal of the Association for Information Systems*, 19(5), 377–407. <https://doi.org/10.17705/1jais.00496>
- Hellgren, J., Sverke, M., & Isaksson, K. (1999). A Two-dimensional Approach to Job Insecurity: Consequences for Employee Attitudes and Well-being. *European Journal of Work and Organizational Psychology*, 8(2), 179–195. <https://doi.org/10.1080/135943299398311>
- Henseler, J., & Sarstedt, M. (2013). Goodness-of-fit indices for partial least squares path modeling. *Computational Statistics*, 28(2), 565–580. <https://doi.org/10.1007/s00180-012-0317-1>
- Henseler, J., Hubona, G., & Ray, P. A. (2016). Using PLS path modeling in new technology research: updated guidelines. *Industrial Management & Data Systems*, 116(1), 2–20. <https://doi.org/10.1108/IMDS-09-2015-0382>
- Hicks, D. (2014). Information technology, change and information professionals' identity construction: A discourse analysis: Information Technology, Change and Information Professionals' Identity Construction: A Discourse Analysis. *Proceedings of the American Society for Information Science and Technology*, 51(1), 1–9. <https://doi.org/10.1002/meet.2014.14505101049>
- Hirschheim, R., & Newman, M. (1988). Information Systems and User Resistance: Theory and Practice. *The Computer Journal*, 31(5), 398–408. <https://doi.org/10.1093/comjnl/31.5.398>
- Hoffman, D. L., & Novak, T. P. (2018). Consumer and Object Experience in the Internet of Things: An Assemblage Theory Approach. *Journal of Consumer Research*, 44(6), 1178–1204. <https://doi.org/10.1093/jcr/ucx105>
- Israeli, T. (2019). Losing information is like losing an arm: employee reactions to data loss. *Behaviour & Information Technology*, 1–11. <https://doi.org/10.1080/0144929X.2019.1662487>
- Jensen, T. B., Kjærgaard, A., & Svejvig, P. (2009). Using Institutional Theory with Sensemaking Theory: A Case Study of Information System Implementation in Healthcare. *Journal of Information Technology*, 24(4), 343–353. <https://doi.org/10.1057/2Fjit.2009.11>
- Johnson, D. G., & Verdicchio, M. (2017). AI Anxiety. *Journal of the Association for Information Science and Technology*, 68(9), 2267–2270. <https://doi.org/10.1002/asi.23867>
- Joshi, K. (1991). A Model of Users' Perspective on Change: The Case of Information Systems Technology Implementation. *MIS Quarterly*, 15(2), 229–242. <https://doi.org/10.2307/249384>
- Jussupow, E., Heinzl, A., & Spohrer, K. (2018). I am; We are - Conceptualizing Professional Identity Threats from Information Technology. *39th International Conference on Information Systems*. Presented at the International Conference On Information Systems.
- Jussupow, E. (2018). Ai Changes Who We Are – Doesn't It? Intelligent Decision Support And Physicians' Professional Identity. *26th European Conference on Information Systems*. Presented at the European Conference On Information Systems.
- Karsten, H., & Laine, A. (2007). User interpretations of future information system use: A snapshot with technological frames. *International Journal of Medical Informatics*, 76, 136–140. <https://doi.org/10.1016/j.ijmedinf.2006.05.013>
- Kim & Kankanhalli. (2009). Investigating User Resistance to Information Systems Implementation: A Status Quo Bias Perspective. *MIS Quarterly*, 33(3), 567–582. <https://doi.org/10.2307/20650309>
- Kock, N. (2015). Common Method Bias in PLS-SEM: A Full Collinearity Assessment Approach. *International Journal of e-Collaboration*, 11(4), 1–10. <https://doi.org/10.4018/ijec.2015100101>
- Krovi, R. (1992). Identifying the causes of resistance to IS implementation: A change theory perspective. *Information & Management*, 25(6), 327–335. [https://doi.org/10.1016/0378-7206\(93\)90082-5](https://doi.org/10.1016/0378-7206(93)90082-5)
- Kühl, N., Lobana, J., & Meske, C. (2019). Do you comply with AI? — Personalized explanations of learning algorithms and their impact on employees' compliance behavior. *48th International Conference on Information Systems*. Presented at the International Conference on Information Systems, Munich.
- Kvale, S., & Brinkmann, S. (2009). *InterViews: Learning the craft of qualitative research interviewing*. SAGE Publications Ltd.
- Lamb, R., & Davidson, E. (2005). Information and Communication Technology Challenges to Scientific Professional Identity. *The Information Society*, 21(1), 1–24. <https://doi.org/10.1080/0197240590895883>
- Laumer, S. (2011). Why do People Reject Technologies - A Literature-based Discussion of the Phenomena "Resistance to Change" in Information Systems and Managerial Psychology Research. *19th European Conference on Information Systems* (p. 13). Presented at the European Conference on Information Systems, Helsinki, Finland.
- Lee, N., & Cadogan, J. W. (2013). Problems with formative and higher-order reflective variables. *Journal of Business Research*, 66(2), 242–247. <https://doi.org/10.1016/j.jbusres.2012.08.004>
- Marabelli, M., Vaast, E., & Li, J. L. (2021). Preventing the digital scars of COVID-19. *European Journal of Information Systems*, 1–17. <https://doi.org/10.1080/0960085X.2020.1863752>

- Marcoulides, & ChinSaunders. (2009). A Critical Look at Partial Least Squares Modeling. *MIS Quarterly*, 33(1), 171–175. <https://doi.org/10.2307/20650283>
- McIntosh, C. N., Edwards, J. R., & Antonakis, J. (2014). Reflections on Partial Least Squares Path Modeling. *Organizational Research Methods*, 17(2), 210–251. <https://doi.org/10.1177/1094428114529165>
- Meissonier, R., & Houzé, E. (2010). Toward an ‘IT Conflict-Resistance Theory’: action research during IT pre-implementation. *European Journal of Information Systems*, 19(5), 540–561. <https://doi.org/10.1057/ejis.2010.35>
- Metaxiotis, K. S. (2000). Expert systems in medicine: Academic illusion or real power? *Information Management*, 8(2), 75–79.
- Meuser, M., & Nagel, U. (2009). The Expert Interview and Changes in Knowledge Production. In A. Bogner, B. Littig, & W. Menz (Eds.), *Interviewing Experts* (pp. 17–42). London: Palgrave Macmillan UK. https://doi.org/10.1057/9780230244276_2
- Mirbabaie, M., Stieglitz, S., Brünker, F., Hofeditz, L., Ross, B., & Frick, N. R. J. (2020). Understanding Collaboration with Virtual Assistants – The Role of Social Identity and the Extended Self. *Business & Information Systems Engineering*, 63(1). <https://doi.org/10.1007/s12599-020-00672-x>
- Mirbabaie, M., Stieglitz, S., & Frick, N. R. J. (2021). Hybrid intelligence in hospitals: towards a research agenda for collaboration. *Electronic Markets*, 31(2). <https://doi.org/10.1007/s12525-021-00457-4>
- Nach, H. (2015). Identity under challenge: Examining user’s responses to computerized information systems. *Management Research Review*, 38(7), 703–725. <https://doi.org/10.1108/MRR-02-2014-0031>
- Neuhofer, B., Magnus, B., & Celuch, K. (2020). The impact of artificial intelligence on event experiences: a scenario technique approach. *Electronic Markets*. <https://doi.org/10.1007/s12525-020-00433-4>
- Ogbanufe, O., & Gerhart, N. (2020). The mediating influence of smart-watch identity on deep use and innovative individual performance. *Information Systems Journal*, 30(6), 977–1009. <https://doi.org/10.1111/isj.12288>
- Okoli, C. (2015). A Guide to Conducting a Standalone Systematic Literature Review. *Communications of the Association for Information Systems*, 37, 879–910. <https://doi.org/10.17705/1CAIS.03743>
- Palan, S., & Schitter, C. (2018). Prolific.ac—A subject pool for online experiments. *Journal of Behavioral and Experimental Finance*, 17, 22–27. <https://doi.org/10.1016/j.jbef.2017.12.004>
- Paré, G., Trudel, M.-C., Jaana, M., & Kitsiou, S. (2015). Synthesizing information systems knowledge: A typology of literature reviews. *Information & Management*, 52(2), 183–199. <https://doi.org/10.1016/j.im.2014.08.008>
- Park, C. S., & Kaye, B. K. (2019). Smartphone and self-extension: Functionally, anthropomorphically, and ontologically extending self via the smartphone. *Mobile Media & Communication*, 7(2), 215–231. <https://doi.org/10.1177/2050157918808327>
- Petriglieri, J. L. (2011). Under Threat: Responses to and the Consequences of Threats to Individuals’ Identities. *Academy of Management Review*, 36(4), 641–662. <https://doi.org/10.5465/amr.2009.0087>
- Petter, S., & Stafford, T. (2017). The Data Base for Advances in Information Systems: A New Editorial Vision. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, 48(1), 7–10. <https://doi.org/10.1145/3051473.3051475>
- Prester, J., Cecez-Kecmanovic, D., & Schlagwein, D. (2019). Becoming a Digital Nomad: Identity Emergence in the Flow of Practice. *48th International Conference on Information Systems*. Presented at the International Conference on Information Systems, Munich.
- Qu, S. Q., & Dumay, J. (2011). The qualitative research interview. *Qualitative Research in Accounting & Management*, 8(3), 238–264. <https://doi.org/10.1108/11766091111162070>
- Rai, A., Constantinides, P., & Sarker, S. (2019). Next-Generation Digital Platforms: Toward Human-AI Hybrids. *MIS Quarterly*, 43(1), iii–x.
- Reinartz, W., Haenlein, M., & Henseler, J. (2009). An empirical comparison of the efficacy of covariance-based and variance-based SEM. *International Journal of Research in Marketing*, 26(4), 332–344. <https://doi.org/10.1016/j.ijresmar.2009.08.001>
- Reychav, I., Beeri, R., Balapour, A., Raban, D. R., Sabherwal, R., & Azuri, J. (2019). How reliable are self-assessments using mobile technology in healthcare? The effects of technology identity and self-efficacy. *Computers in Human Behavior*, 91, 52–61. <https://doi.org/10.1016/j.chb.2018.09.024>
- Ringle, C. M., Wende, S., & Becker, J. M. (2020). *SmartPLS3*. Boenningstedt.
- Ringle, Sarstedt, & Straub. (2012). Editor’s Comments: A Critical Look at the Use of PLS-SEM in “MIS Quarterly.” *MIS Quarterly*, 36(1), iii. <https://doi.org/10.2307/41410402>
- Russel, S., & Norvig, P. (2016). *Artificial Intelligence: A Modern Approach*. Addison Wesley.
- Ryan, G. W., & Bernard, H. R. (2003). Techniques to Identify Themes. *Field Methods*, 15(1), 85–109. <https://doi.org/10.1177/1525822X02239569>
- Sarstedt, M., Hair, J. F., Ringle, C. M., Thiele, K. O., & Gudergan, S. P. (2016). Estimation issues with PLS and CBSEM: Where the bias lies! *Journal of Business Research*, 69(10), 3998–4010. <https://doi.org/10.1016/j.jbusres.2016.06.007>
- Schilling, J. (2006). On the Pragmatics of Qualitative Assessment. *European Journal of Psychological Assessment*, 22(1), 28–37. <https://doi.org/10.1027/1015-5759.22.1.28>
- Schweitzer, F., Belk, R., Jordan, W., & Ortner, M. (2019). Servant, friend or master? The relationships users build with voice-controlled smart devices. *Journal of Marketing Management*, 35(7–8), 693–715. <https://doi.org/10.1080/0267257X.2019.1596970>
- Selz, D. (2020). From electronic markets to data driven insights. *Electronic Markets*, 30(1), 57–59. <https://doi.org/10.1007/s12525-019-00393-4>
- Shin, D. (2021). The effects of explainability and causability on perception, trust, and acceptance: Implications for explainable AI. *International Journal of Human-Computer Studies*, 146, 102551. <https://doi.org/10.1016/j.ijhcs.2020.102551>
- Shmueli, G., & Koppius, O. (2011). Predictive Analytics in Information Systems Research. *MIS Quarterly*, 35(3), 553–572. <https://doi.org/10.2307/23042796>
- Shrestha, Y. R., Ben-Menahem, S. M., & von Krogh, G. (2019). Organizational Decision-Making Structures in the Age of Artificial Intelligence. *California Management Review*, 61(4), 66–83. <https://doi.org/10.1177/0008125619862257>
- Siau, K., & Wang, W. (2018). Building Trust in Artificial Intelligence, Machine Learning, and Robotics. *Cutter Business Technology Journal*, 31(2), 47–53.
- Silva, L., Hsu, C., Backhouse, J., & McDonnell, A. (2016). Resistance and power in a security certification scheme: The case of c:cure. *Decision Support Systems*, 92, 68–78. <https://doi.org/10.1016/j.dss.2016.09.014>
- Sime, J.-A., & Themelis, C. (2020). Educators’ perspectives on trans-media identity management: redefining tele-teacher presence. *Distance Education*, 41(1), 70–85. <https://doi.org/10.1080/01587919.2020.1727292>
- Stein, M.-K., Galliers, R. D., & Markus, M. L. (2013). Towards An Understanding of Identity and Technology in the Workplace. *Journal of Information Technology*, 28(3), 167–182. <https://doi.org/10.1057/jit.2012.32>

- Stein, J.-P., Liebold, B., & Ohler, P. (2019). Stay back, clever thing! Linking situational control and human uniqueness concerns to the aversion against autonomous technology. *Computers in Human Behavior*, 95, 73–82. <https://doi.org/10.1016/j.chb.2019.01.021>
- Stets, J. E., & Burke, P. J. (2000). Identity Theory and Social Identity Theory. *Social Psychology Quarterly*, 63(3), 224. <https://doi.org/10.2307/2695870>
- Stone, M. (1974). Cross-validatory choice and assessment of statistical predictions. *Journal of the Royal Statistical Society*, 36(2), 111–147.
- Strauss, A., & Corbin, J. M. (1990). *Basics of qualitative research: Grounded theory procedures and techniques*. Sage Publications, Inc.
- Sun, Y., Wang, N., & Shen, X.-L. (2020). Toward a Configurational Protection Motivation Theory. *Proceedings of the 53rd Hawaii International Conference on System Sciences* (pp. 3597–3606). Presented at the Hawaii International Conference on System Sciences, Maui, Hawaii. <https://doi.org/10.24251/HICSS.2020.440>
- Sundar, S. S. (2020). Rise of Machine Agency: A Framework for Studying the Psychology of Human–AI Interaction (HAI). *Journal of Computer-Mediated Communication*, 25(1), 74–88. <https://doi.org/10.1093/jcmc/zmz026>
- Svejvig, P., & Jensen, T. B. (2012). Making sense of enterprise systems in institutions: A case study of the re-implementation of an accounting system. *Scandinavian Journal of Information Systems*, 25(1), 3–36.
- Tenenhaus, M., Vinzi, V. E., Chatelin, Y.-M., & Lauro, C. (2005). PLS path modeling. *Computational Statistics & Data Analysis*, 48(1), 159–205. <https://doi.org/10.1016/j.csda.2004.03.005>
- Teubner, R. A. (2007). Strategic information systems planning: A case study from the financial services industry. *The Journal of Strategic Information Systems*, 16(1), 105–125. <https://doi.org/10.1016/j.jsis.2007.01.002>
- Thiebes, S., Lins, S., & Sunyaev, A. (2021). Trustworthy artificial intelligence. *Electronic Markets*, 31(2). <https://doi.org/10.1007/s12525-020-00441-4>
- Utesheva, A., Simpson, J. R., & Cecez-Kecmanovic, D. (2016). Identity metamorphoses in digital disruption: a relational theory of identity. *European Journal of Information Systems*, 25(4), 344–363. <https://doi.org/10.1057/ejis.2015.19>
- Vaast, E., Davidson, E. J., & Mattson, T. (2013). Talking about Technology: The Emergence of a New Actor Category Through New Media. *MIS Quarterly*, 37(4), 1069–1092. <https://doi.org/10.25300/MISQ/2013/37.4.04>
- Venkatesh, V. (2021). Adoption and use of AI tools: a research agenda grounded in UTAUT. *Annals of Operations Research*. <https://doi.org/10.1007/s10479-020-03918-9>
- vom Brocke, J., Simons, A., Riemer, K., Niehaves, B., Plattfaut, R., & Cleven, A. (2015). Standing on the Shoulders of Giants: Challenges and Recommendations of Literature Search in Information Systems Research. *Communications of the Association for Information Systems*, 37(9), 205–224. <https://doi.org/10.17705/1CAIS.03709>
- Walsham, G. (1998). IT and changing professional identity: Micro-studies and macro-theory. *Journal of the American Society for Information Science*, 49(12), 1081–1089.
- Wang, W., & Siau, K. (2019). Artificial Intelligence, Machine Learning, Automation, Robotics, Future of Work and Future of Humanity: A Review and Research Agenda. *Journal of Database Management*, 30(1), 61–79. <https://doi.org/10.4018/JDM.2019010104>
- Webster, J., & Watson, R. T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Quarterly*, 26(2), xii–xxiii.
- Wetzels, Odekerken-Schröder, & van Oppen. (2009). Using PLS Path Modeling for Assessing Hierarchical Construct Models: Guidelines and Empirical Illustration. *MIS Quarterly*, 33(1), 177. <https://doi.org/10.2307/20650284>
- Wirtz, B. W., Weyerer, J. C., & Sturm, B. J. (2020). The Dark Sides of Artificial Intelligence: An Integrated AI Governance Framework for Public Administration. *International Journal of Public Administration*, 43(9), 818–829. <https://doi.org/10.1080/01900692.2020.1749851>
- Yang, Y., & Siau, K. L. (2018). A Qualitative Research on Marketing and Sales in the Artificial Intelligence Age. *MWAIS 2018 Proceedings*. Presented at the Midwest Association for Information Systems Conference, Saint Louis, Missouri.
- Zhang, B., & Dafoe, A. (2019). Artificial Intelligence: American Attitudes and Trends. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3312874>
- Złotowski, J., Yogeewaran, K., & Bartneck, C. (2017). Can we control it? Autonomous robots threaten human identity, uniqueness, safety, and resources. *International Journal of Human-Computer Studies*, 100, 48–54. <https://doi.org/10.1016/j.ijhcs.2016.12.008>

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.