Received: 21 March 2020 | Revised: 24 March 2022 | Accepted: 3 April 2022

DOI: 10.1111/isj.12386

RESEARCH ARTICLE

WILEY

The multidimensional nature of privacy risks: Conceptualisation, measurement and implications for digital services

Sabrina Karwatzki[1] | Manuel Trenz[2] | Daniel Veit[1]

[1]Faculty of Business and Economics, University of Augsburg, Augsburg, Germany

[2]Faculty of Business and Economics, University of Goettingen, Goettingen, Germany

Correspondence
Daniel Veit, Faculty of Business and Economics, University of Augsburg, Universitaetsstrasse 16, D-86159 Augsburg, Germany.
Email: daniel.veit@uni-a.de

Abstract

While today consumers benefit from personalised service offerings, they are also understandably concerned about the privacy risks generated by disclosing their personal information online. We know that such perceived risks in general shape behaviour, but we know little about what specific privacy risks obstruct the use of digital services, making it difficult to implement technologies that could mitigate these risks. Based on qualitative and quantitative studies involving over 1000 participants, we conceptualise and quantify a multidimensional perspective on privacy risks consisting of physical, social, resource-related, psychological, prosecution-related, career-related and freedom-related privacy risks. Our results explicate the prospects of distinguishing privacy risk dimensions by demonstrating how they are differently pronounced across contexts and how technology designs can be tailored to assuage them. Thus, our findings improve the understanding of context and service-specific privacy risks, helping managers to adjust their digital offerings to mitigate users' privacy risk perceptions.

KEYWORDS
information privacy, privacy risk, privacy risk dimensions, risk mitigation, scale development, service design

Sabrina Karwatzki and Manuel Trenz contributed equally to this work.

1 | INTRODUCTION

Information from users or customers constitutes a key factor in the innovation and success of firms (Abbasi et al., 2016; Savage, 2020). However, disclosing their personal information can have potentially adverse consequences for these individuals (Acquisti et al., 2015; Kordzadeh & Warren, 2017). When making decisions concerning the use of digital service and disclosure of personal information, individuals wonder 'What could happen to me if this information about me were accessible to others?' (Karwatzki, Trenz, et al., 2017). Recent surveys suggest that the spectrum of information privacy[1] risks individuals perceive is very broad, including for example, unwanted marketing influence, feelings of constant surveillance and discrimination by third parties (European Commission, 2016; KPMG, 2016; TRUSTe, 2016). If the perceived privacy risks are too high, individuals will not use digital services or will refrain from providing information that allows firms to provide, personalise and ultimately monetise their services (Chellappa & Sin, 2005; Sutanto et al., 2013).

Understanding the diversity of individuals' privacy risks is important for all stakeholders. From the individual's perspective, for example, the risk of being discriminated against is of a very different nature than the risk of being influenced by marketing. Therefore, these different privacy risks will most likely require different mitigating actions from firms or policy makers. Thus, for firms, it is of utmost importance to understand the specific nature of the privacy risks their prospective users associate with their services in order to be able to mitigate them. Along the same lines, if governments do not understand what privacy risks individuals associate with particular digital innovations (Trang et al., 2020), they may also fail to use them to address societal challenges such as the coronavirus disease 2019 (COVID-19) pandemic. Lastly, a nuanced understanding of individuals' privacy risks is also crucial for policy makers to put regulations in place to protect citizens.

Although much extant research does acknowledge the importance of understanding privacy perceptions, prior studies fail to cater to the above-mentioned need as they do not link those perceptions to particular consequences for individuals that could be prevented or mitigated by design or policy decisions. One significant stream of privacy research emphasises the importance of privacy risks. Privacy risks are generally associated with either the potential for opportunistic behaviour by third parties having access to an individual's information (Dinev & Hart, 2006; van Slyke et al., 2006; Wu et al., 2009; C. Xu et al., 2015) or the belief in a potential for loss caused by an individual's disclosure of personal information (Libaque-Sáenz et al., 2021; Liu et al., 2019; Malhotra et al., 2004; H. Xu et al., 2009). However, these privacy risks are conceptualised as a unidimensional construct that refers to a general potential for loss when personal information is available to other parties, without specifying the nature or cause of the loss. While unidimensional privacy risks help determine *whether* individuals associate the potential of a loss with information access by third parties, they do not yet provide tangible insights into the nature of this risk.

Another stream of privacy research focusses on the concept of privacy concerns – defined as the worries that individuals have regarding how their personal information is handled by others (Hong & Thong, 2013; Smith et al., 1996). This stream of research has acknowledged the importance of multidimensional privacy constructs by distinguishing between perceptions of different organisational practices such as data collection, secondary usage or errors (Hong & Thong, 2013) or between peer privacy violations (Zhang et al., 2022). Measuring privacy concerns this way allows a fine-grained understanding of individuals' perceptions of other party's behaviour, even though it remains unclear whether and why such behaviour of others would be associated with significant negative consequences for the individual.

The importance of information privacy has also given rise to other constructs for assessing situational privacy perceptions such as privacy invasion (Ayyagari & Grover, 2011), privacy awareness (H. Xu et al., 2011), privacy uncertainty (Al-Natour et al., 2020), privacy control (Krasnova et al., 2010) and privacy protection (Kim et al., 2008). Others refer to individual characteristics such as privacy knowledge (Crossler & Bélanger, 2019), privacy self-efficacy (Crossler & Bélanger, 2019), privacy experience (Ozdemir et al., 2017) or the disposition to value privacy (H. Xu et al., 2011). Although studies using these constructs help uncover *whether* and *under what conditions* privacy is a key concern for individuals, they are also either unidimensional or focus on organisational practices and therefore do

not yield insights into what particular risks individuals perceive. As a result, we lack an understanding of the nature of privacy risks across different digital services and settings.

Interestingly and importantly, it is negative personal consequences that trigger behavioural change (Dowling, 1986) and changes in perceived privacy risks are instrumental to actual choices (Adjerid et al., 2018). Therefore, measuring and understanding what privacy risks individuals associate with specific digital services and innovations may be key to successfully obtaining personal information with individuals' consent and therefore to the competitiveness of data-driven businesses. To address this issue, we propose to decompose the general concept of privacy risks into its constituting dimensions and develop a measurement model to assess them.

In addition to the practical implications of assuaging customers' risk perceptions and increasing business competitiveness, a multidimensional account of privacy risks has the potential to advance theory by allowing researchers to develop more concise explanations of how comprehensive concepts are linked to existing nomological networks (Law et al., 1998). It would enable us to move from assessing the level of privacy risks towards understanding the nature of privacy risks given a certain situation. Insights derived from specific risk dimensions outside of the privacy domain have proven valuable in information systems (IS) research (Featherman & Pavlou, 2003; Luo et al., 2010) and other disciplines such as marketing (Stone & Grønhaug, 1993) and travel research (Park & Tussyadiah, 2017). Acknowledging and evaluating multiple dimensions of privacy risks would allow researchers to zoom in and increase the realism in empirical models (Edwards, 2001) while providing a comparatively simple abstraction for a complex concept (Polites et al., 2012).

Given firms' dependency on user information on the one hand, and their struggle to pinpoint and mitigate users' actual privacy-related fears on the other, we argue that it is critically important to determine the exact nature of the specific consequences individuals fear when others have access to their personal information.

Based on these considerations, we pose the following research question:

> What is a multidimensional conceptualisation of privacy risks and how can its assessment advance the understanding and management of privacy risks?

To address this question, we conduct the following research process and structure this paper accordingly. We first build upon multidimensional risk concepts outside of the privacy domain as well as studies on privacy-related adverse consequences to conceptualise multidimensional privacy risks consisting of seven specific privacy risks associated with access to personal information. We then conduct an extensive scale development process (MacKenzie et al., 2011) to derive reliable and valid measurement scales facilitating the assessment of digital services in relation to the nature of specific perceived privacy risks. We illustrate the validity and importance of our multidimensional conceptualisation of privacy risks and the associated measurement scales through four quantitative studies involving 1086 individuals. We conduct two pretests to refine the measurement scales and then two main studies. Main study 1 evaluates multidimensional privacy risks in a nomological network and investigates the contextual differences of privacy risk perceptions across dimensions. Main study 2 looks at how to mitigate specific privacy risk dimensions through technology and service design. Finally, we discuss our results, both theoretical and practical contributions, as well as avenues for future research.

Our study contributes to extant research in five ways. First, we disentangle the previously aggregated concept of privacy risks into seven distinct dimensions. Despite the unquestioned importance of privacy risks (Adjerid et al., 2018), the manifold studies on privacy risks treat it as an aggregate concept, which is in stark contrast to the complex nature of risks uncovered in domains other than information privacy (Featherman & Pavlou, 2003; Glover & Benbasat, 2010; Luo et al., 2010). By unfolding this black box of privacy risks, our rich conceptualisation of privacy risks opens up avenues for a deeper understanding of information privacy (Polites et al., 2012). Second, following state-of-the-art procedures (MacKenzie et al., 2011), we develop a reliable and valid measurement instrument for multidimensional privacy risks. The instrument has been tested qualitatively and quantitatively, within a nomological network, across contexts, and has proven valuable in experimental manipulation. The ability to measure individual

privacy risks is the prerequisite for deriving a more fine-grained understanding of privacy considerations across contexts and for offering relevant actionable design advice for digital services; from *'both practical and research standpoints, what cannot be measured cannot be managed'* (Hille et al., 2015, p. 2). As a result, it allows researchers to study multidimensional privacy risks within their particular area of interest and thereby accelerates academic progress within the domain of information privacy. Third, we contribute to the call for contextualisation in information systems research (Avgerou, 2019) by providing a first indication on how the nature of privacy risks may differ across contexts. We thereby showcase how multidimensional privacy risks can help in deriving a more realistic and complete view of privacy perceptions across contexts. Fourth, we advance prior research on privacy design by showing that designing for privacy does not necessarily influence privacy risks in general. Instead, we show that selected design features are more powerful in mitigating some dimensions of privacy risks than others. Thereby, we facilitate the design of data-intense services to tailor their features in a way that more effectively mitigates those privacy risks that users actually care about. Last, our article is one of the few that has exercised and documented all of the scale development steps as suggested by MacKenzie et al. (2011). In particular, we pay special attention to the often neglected aspect of veridicality of the measurement instrument. As such, it may be helpful to future researchers attempting to develop a new measurement instrument.

2 | THEORETICAL BACKGROUND AND RELATED LITERATURE

Information privacy – defined as 'an individual's self-assessed state in which external [parties] have limited access to information about him or her' (Dinev et al., 2013, p. 299) – is an important concept in IS research (Bélanger & Crossler, 2011). IS researchers are interested in understanding the impact of digital services in specific and information technologies in general on the control individuals have over the collection and use of their personal information.

In this study, we are searching for a way to understand and capture the multidimensional nature of privacy risks. Therefore, in this section, we review existing concepts to capture privacy and investigate risk dimensions beyond the privacy and IS domains. Then, as existing knowledge on the dimensions of privacy risks is scarce, we apply a taxonomical approach to synthesise the privacy-related adverse consequences as a building block for our conceptualisation of multidimensional privacy risks.

2.1 | Key concepts to capture privacy

Because privacy is difficult to measure directly, empirical research relies on privacy-related proxies. While the common convention is to use privacy concerns and privacy risks as central constructs (Smith et al., 2011), many other privacy constructs have also developed over time. We describe all these approaches below and explain why they are not suitable for a deeper understanding and measurement of individuals' perceptions of negative outcomes that may arise from others' access to their personal information – which is the focus of this study.

Two established operationalisations for *privacy concerns* exist. The first is the 'concern for information privacy' scale (Smith et al., 1996), which differentiates between four privacy concern dimensions: the concern that personal data are collected, is internally or externally used in an unauthorised way, is improperly accessed or is erroneous. The second is the 'internet users' information privacy concerns' scale (Malhotra et al., 2004), which includes users' concerns about information collection, users' control over the collected information and the users' awareness of how the information is used. Hong and Thong (2013) conceptualise and integrate these two operationalisations into one measurement instrument. Overall, privacy concerns are conceptualised to focus on individuals' perceptions of how organisations handle their data. The research stream has benefitted strongly from multidimensional perspectives on privacy concerns, which have allowed researchers to analyse organisational practices concerning privacy in a much more nuanced way. Acknowledging the multitude of external parties that may threaten individuals' privacy, Zhang

et al. (2022) propose a novel multidimensional privacy concerns construct that focusses on peer interactions rather than organisational practices. However, these conceptualisations do not consider individuals' perceptions of whether and how such organisational or peer practices may negatively impact them personally – which is what we want to investigate in this study.

Conceptualisations of *privacy risks* can be broadly divided into two classes. First, privacy risks have been conceptualised as the fear that other parties, authorised or unauthorised, may behave opportunistically if they gain access to an individual's personal information (Dinev & Hart, 2006; van Slyke et al., 2006; Wu et al., 2009). This conceptualisation is similar to the one of privacy concerns in that neither focusses directly on the specific negative consequences that could arise from such opportunistic behaviour. Second, privacy risks have been defined as the belief that there is a high potential for loss if an individual's information is disclosed to other parties (Malhotra et al., 2004; Smith et al., 2011; H. Xu et al., 2009). Such instruments assess the levels of perceived privacy risks but remain abstract with regards to the actual losses or consequences that may occur (Dinev & Hart, 2006; H. Xu et al., 2009). A detailed investigation of different privacy risk conceptualisations testifies to the wide use of this privacy risk perspective but also shows the prevalence of its unidimensionality (see Appendix A, Supporting information). However, losses associated with privacy risks can take diverse forms and such unidimensional conceptualisations of a potentially multidimensional construct leave plenty of space for ambiguity and interpretation (Converse & Presser, 1986). For example, in an online shopping context, individuals may risk financial losses if their credit card data are abused, while in a social networking context, the primary fear may be reputational damage. Existing conceptualisations fail to depict the complexity of real-life risk situations. They do not provide a contextualised, privacy-specific understanding of risk, which would be helpful in two ways: it could be useful for individuals, organisations and policy makers seeking to understand how individuals assess specific situations in which a loss of privacy may occur and it could offer guidance for possible interventions.

Beyond the above two most-prevalent perspectives, the growing body of literature on privacy has also given rise to a multitude of concepts and constructs, all of them serving unique purposes when studying privacy phenomena. The concepts range from contextual evaluations (privacy awareness, privacy control, privacy invasion, privacy uncertainty), to personality traits (disposition to value privacy), to prior experiences (privacy experience), to expectations (privacy protection) and to expertise and skills (privacy knowledge, privacy self-efficacy). While these concepts and constructs have proven valuable in facilitating our understanding of this crucial topic, they are less useful in capturing the nature of privacy risks as none of them refers to specific consequences of others' access to personal information or the specific privacy risks individuals perceive. All these constructs – along with their definitions, purposes and attributes – are summarised in Appendix B (Supporting information).

In conclusion, when looking at existing privacy conceptualisations, three key observations arise. First, there is an uninterrupted demand for elaborate concepts that capture the complexity of phenomena related to information privacy. Second, privacy risks are a central concept for explaining behavioural reactions in the area of information privacy. Third, despite the value and diffusion of multidimensional privacy concepts (particularly with regards to organisational practices), prior studies do not cater to the need of disentangling individuals' perceptions of privacy risks and the privacy-related adverse consequences. As a result, we turn to the literature on risk dimensions outside of the privacy and IS domain.

2.2 | Privacy-related adverse consequences as a component of privacy risks

As existing privacy-related conceptualisations and measurement instruments do not provide insights into specific privacy risks, we take a look at risks outside of the privacy context. *Risks* have been commonly defined as consisting of two components: (1) the severity of negative consequences of a situation and (2) their probability of occurrence (Cunningham, 1967; Dowling, 1986; Jacoby & Kaplan, 1972; Mitchell, 1999). These two components also need to be reflected in a privacy risk conceptualisation.

Moreover, multidimensional risk perspectives are widely used outside the privacy context (Dowling, 1986). In marketing and e-commerce, for example, risks are generally defined as multidimensional (Dowling, 1986); their risk dimensions refer to specific negative outcomes, such as performance, financial, social, physical and psychological adverse consequences (Cunningham, 1967; Dowling, 1986; Glover & Benbasat, 2010; Jacoby & Kaplan, 1972). The aforementioned risk dimensions identified in other research contexts suggest several possible dimensions for the current project, but they must be adapted and extended to align with the unique negative consequences that could characterise dimensions of privacy risks. In fact, privacy risks do not refer to risks regarding product quality or online transactions; rather, they assess the perceived consequences of information misuse and their likelihood of occurrence.

While prior literature has not distinguished between specific dimensions of privacy risks, few prior studies on privacy have touched upon specific privacy-related adverse consequences, one essential component of privacy risks. The privacy-related consequences comprise unwanted marketing ads, home burglary, financial losses, price discrimination or other economic discrimination (Acquisti et al., 2015; Chen & Sharma, 2013; Crossler & Posey, 2017; Degirmenci et al., 2013; Featherman & Pavlou, 2003; Haug et al., 2020; Kordzadeh & Warren, 2017; Krasnova et al., 2010; T. Li & Unger, 2012; Miltgen & Smith, 2015; Smith et al., 2011; Treiblmaier & Pollach, 2007; van Slyke et al., 2006; G. Walsh et al., 2018; Yaraghi et al., 2019), adverse physical consequences such as physical stalking or lower quality health care (Kordzadeh & Warren, 2017; Smith et al., 2011; Yaraghi et al., 2019) – as well as different facets of social consequences, such as embarrassment, harassment and bullying (Krasnova et al., 2010; T. Li & Unger, 2012; Ozdemir et al., 2017), cyber stalking and reputation damage (Chen & Sharma, 2013; Kordzadeh & Warren, 2017; Miltgen & Smith, 2015; G. Walsh et al., 2018; H. Xu et al., 2008), social sanctions (Acquisti et al., 2015; Lanzing, 2019) and stigmatisation of illness (Yaraghi et al., 2019). These consequences are in line with financial, physical and social risk dimensions found in other contexts and yet describe privacy-specific manifestations.

A few studies touching upon privacy-related adverse consequences have also named consequences that have not been encountered in contexts outside the privacy area. These include for instance hidden influence and manipulation (Acquisti et al., 2015), job-related fears (Kordzadeh & Warren, 2017; Krasnova et al., 2010; Lanzing, 2019; Schmoll & Bader, 2019; Yaraghi et al., 2019), feelings of uneasiness and powerlessness due to surveillance, censorship and loss of control (Acquisti et al., 2015; Crossler & Posey, 2017; Degirmenci et al., 2013; Haug et al., 2020; Kordzadeh & Warren, 2017; T. Li & Unger, 2012; Schmoll & Bader, 2019; Smith et al., 2011; Treiblmaier & Pollach, 2007; Yaraghi et al., 2019), criminal prosecution (Kordzadeh & Warren, 2017) and interference with the decision-making process (Lanzing, 2019). However, all these studies only name these potential consequences; besides social and resource-related consequences, none of the consequences is conceptualised in depth.

A notable exception is the study by Karwatzki, Trenz, et al. (2017). They conducted qualitative research in terms of an exploratory focus group study with 119 participants in 22 focus groups. The focus group discussions aimed to uncover a broad range of adverse consequences across different contexts that may arise if someone has access to personal information. All focus group sessions were recorded and transcribed, and an iterative analysis using open and axial coding was conducted. As a result, Karwatzki, Trenz, et al. (2017) identify seven dimensions of adverse consequences that describe how privacy-invasive practices such as data collection, improper access or unauthorised usage might impact individuals. These consequences can provide us with an understanding of how the abstract notion of a 'loss of privacy' may manifest in the following respective ways: reduced levels of physical safety, a negative change in individual's social relationships, loss of resources such as time or money, less peace of mind, legal actions taken against individuals, negative career impacts and restricted freedom of opinion and behaviour (Karwatzki, Trenz, et al., 2017).

To get an encompassing view on all privacy-related adverse consequences presented in prior literature, we followed a taxonomical approach to abstract from the specific exemplary privacy consequences. Following the empirical-to-conceptual approach of Nickerson et al. (2013), we identified commonalities of the consequences. We then used these common characteristics to group the consequences and thereby identify seven privacy-specific

TABLE 1 Privacy-related adverse consequences

Source	Identification of consequences	Nature of consequences						
		Physical	Social	Resource-related	Psychological	Prosecution-related	Career-related	Freedom-related
Acquisti et al. (2015)	Exemplarily named, no conceptualisation		x	x	x			x
Chen and Sharma (2013)	Exemplarily named, no conceptualisation		x	x				
Crossler and Posey (2017)	Exemplarily named, no conceptualisation			x	x			
Degirmenci et al. (2013)	Exemplarily named, no conceptualisation			x	x			
Featherman and Pavlou (2003)	Exemplarily named, no conceptualisation			x				
Haug et al. (2020)	Exemplarily named, no conceptualisation			x	x			
Karwatzki, Trenz, et al. (2017)	Empirical: Focus groups used to uncover the different types of adverse consequences that may arise from access to someone's information	x	x	x	x	x	x	x
Kordzadeh and Warren (2017)	Exemplarily named, no conceptualisation	x	x	x	x	x	x	
Krasnova et al. (2010)	Exemplarily named, no conceptualisation		x	x			x	
Lanzing (2019)	Conceptualisation of interference with a person's or group's decision-making process		x	x			x	x
T. Li and Unger (2012)	Exemplarily named, no conceptualisation		x	x	x			
Miltgen and Smith (2015)	Conceptualisation of identity and financial fraud concerns		x	x				
Ozdemir et al. (2017)	Conceptualisation of social consequences		x					
Schmoll and Bader (2019)	Exemplarily named, no conceptualisation				x		x	
Smith et al. (2011)	Exemplarily named, no conceptualisation	x		x	x			
Treiblmaier and Pollach (2007)	Exemplarily named, no conceptualisation			x	x			
van Slyke et al. (2006)	Exemplarily named, no conceptualisation			x				
G. Walsh et al. (2018)	Conceptualisation of fear of financial losses and fear of reputational damage		x	x				
H. Xu et al. (2008)	Exemplarily named, no conceptualisation		x					
Yaraghi et al. (2019)	Exemplarily named, no conceptualisation	x	x	x	x		x	

dimensions: physical, social, resource-related, psychological, prosecution-related, career-related and freedom-related consequences. The focus was set on deriving dimensions that comprise characteristics that are mutually exclusive and collectively exhaustive. At the same time, the resulting categorisation needed to be parsimonious and contain as few dimensions as necessary to be easy to comprehend and apply (Nickerson et al., 2013).

The result of our taxonomical approach is in line with the findings by Karwatzki, Trenz, et al. (2017) and can be found in Table 1. It represents the mapping of the different consequences found in the literature to the seven privacy-specific dimensions identified.

In summary, our investigation of general risk conceptualisations indicates that adverse consequences are an essential component of risk in general, which is also the case for privacy risk. Prior studies suggested that the consequences that individuals are afraid of in the context of information privacy differ significantly from those relevant to product evaluations or online transactions. At the same time, we were able to synthesise prior conceptual and empirical work on privacy-specific adverse consequences to extract the aforementioned seven dimensions of privacy-specific adverse consequences. Besides many studies mentioning selected adverse consequences, the existing empirical work by Karwatzki, Trenz, et al. (2017) provides valuable insights into the manifestations of different privacy-related adverse consequences, illustrative quotes and examples that can inform our work towards a multidimensional privacy risk conceptualisation. The seven adverse consequences identified serve as a starting point for theorising multidimensional privacy risks and developing a scale to assess them.

3 | MULTIDIMENSIONAL PRIVACY RISKS

In the progress towards our research goal, we first conceptualise privacy risks, taking its constituent dimensions into account. We then develop and validate scales for assessing multidimensional privacy risks. Using these newly developed scales, we aim to demonstrate that individuals differ in their risk assessments across different situations and that their risk perceptions can be experimentally influenced, for example, by technology design. More specifically, we argue that the multidimensional conceptualisation (as compared to aggregated measures) of privacy risks allows for a more fine-grained assessment of the nature of privacy risks, and that this deeper understanding is of great importance for effective risk mitigation through technology design.

We followed the approach of MacKenzie et al. (2011) to generate, validate and refine our measurement instrument. Figure 1 depicts the essential activities and outcomes of our five-step scale-development process, which we discuss in detail below.

3.1 | Step 1: Conceptualisation

The first step of the scale development and validation process is to develop a conceptual definition of the construct. MacKenzie et al. (2011) highlight the importance of specifying not only the nature of a construct in terms of the property it represents and the entity to which it applies but also the conceptual theme of the construct by outlining its characteristics, dimensionality and stability. This first step is crucial because failure to precisely specify the construct threatens its validity (MacKenzie et al., 2011).

To conceptualise multidimensional privacy risks, we contextualise the general risk definition to the privacy area. As outlined in the previous section, risks have been commonly defined as consisting of two components: (1) the severity of adverse consequences of a situation and (2) their probability of occurrence (Cunningham, 1967; Dowling, 1986; Jacoby & Kaplan, 1972; Mitchell, 1999). We thus define *privacy risks* as *the extent to which an individual believes that negative outcomes may arise from others' access to his or her personal information*. The accessing entity can here be known or unknown, authorised or unauthorised (Yun et al., 2019). This construct refers to a perception because it describes the individually perceived risk in a specific situation. Moreover, the multidimensional construct

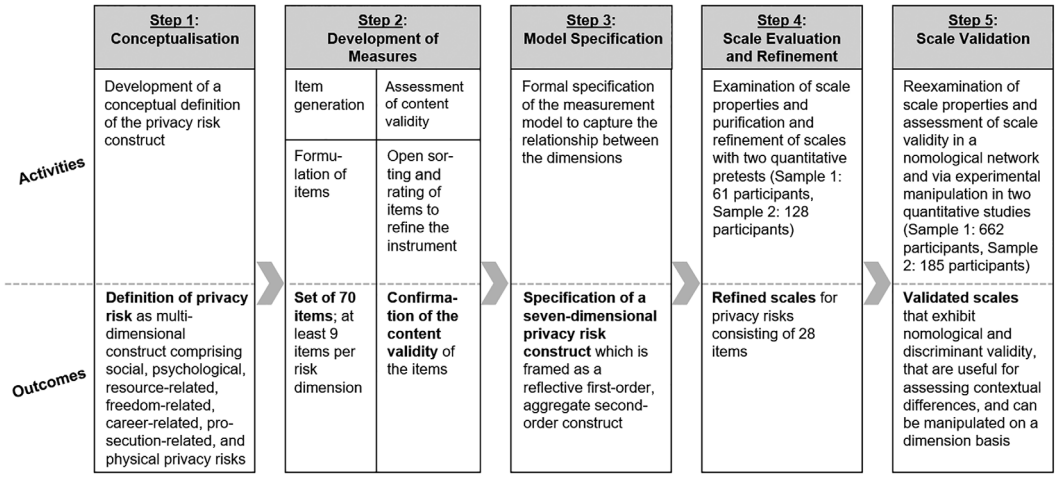

FIGURE 1 Scale development process (adapted from MacKenzie et al., 2011)

of privacy risks applies to the entity of individuals. It is not intended to measure the privacy risks of groups or organisations because these parties likely face different risk dimensions.

In Section 2, we outlined the current status of literature on privacy-related adverse consequences. Our taxonomical approach revealed seven distinct consequences, namely, physical, social, resource-related, psychological, prosecution-related, career-related and freedom-related adverse consequences. We expand these seven consequences by the second component of risk – that is, its probability of occurrence – to arrive at a concept that covers privacy risk in its entirety. In this case, the probability of occurrence is characterised by an individual's subjective assessment of how likely it is that a specific consequence may occur in a specific setting. The combination of consequences and perceived probabilities yields a multidimensional privacy risk concept comprising the seven dimensions of physical, social, resource-related, psychological, prosecution-related, career-related and freedom-related privacy risks.

Physical privacy risks are concerned with negative physical consequences (such as stalking or physical violence) that may arise when information about individuals' habits and physical whereabouts is misused. Individuals have beliefs on the probability of the occurrence of these physical consequences arising from others' access to their information, shaping physical privacy risks. In the same fashion, *social privacy risks* describe individuals being afraid of their social relationships being negatively affected when others get access to personal information. For example, individuals believe that others might form a dismissive opinion about them or social conflicts might arise due to information about one's opinions, lifestyle or behaviour. Again, the evaluation of specific adverse consequences that may arise as well as beliefs in their probability of occurrence manifest in the dimension social privacy risks. If individuals fear that they may have to deal with deleting spam emails, misuse of their payment details or burglary of tangible goods, these are examples of loss of temporal, financial or material resources due to information abuse; individuals' assessment of such risks is captured by the category of *resource-related privacy risks*. Negative psychological consequences comprise the mental discomfort caused by surveillance or a loss of control. Individuals' fears of the occurrence of these consequences result in *psychological privacy risks*, which can be defined as the risk that an individual's peace of mind may be negatively affected as a result of others' having access to personal information. *Prosecution-related privacy risks* describe individuals' fears that personal information might be used to take legal actions against them, regardless of whether they are actually guilty (in case an individual is held liable for illegal activities he or she performed) or just falsely accused (as in case of identity theft or false suspicion). When individuals are afraid that others having access to their personal information might negatively impact their career, we speak of *career-related privacy risks*. Individuals may for example be afraid that employers will get access to information that will lead them to believe that they are

TABLE 2 Dimensions of privacy risks

Dimension	Definition: The extent to which an individual believes that...	Example
Physical privacy risk	... a loss of physical safety may arise from access to his/her information.	A woman believes that posting details (such as GPS tracking and lap times) about her every morning jog in the woods on a social media site could make her vulnerable to assault.
Social privacy risk	... a change in an individual's social status may arise from access to his/her information.	A teenager believes that sharing details on his favourite movies and leisure activities may lead to others bullying him.
Resource-related privacy risk	... a loss of resources may arise from access to his/her information.	A person believes that an insurance company might access her search history on Google to learn which diseases she has researched extensively in the past. She believes that they might assume that she has these diseases and then classify her accordingly in the insurance policy.
Psychological privacy risk	... a negative impact on his/her peace of mind may arise from access to his/her information.	An individual feels awkward about disclosing information about his daily life using instant messaging because he is afraid of surveillance and does not know what all this information could be used for in the future.
Prosecution-related privacy risk	... legal actions against him/her may arise from access to his/her information.	A man is afraid of identity theft when paying online with his credit card. He believes that his identity and payment information could be misused to access illegal content such as child pornography and that he may be held liable for that in the future.
Career-related privacy risk	... negative impacts on his/her career may arise from access to his/her information.	During her teenage years, a woman was in psychological treatment due to her bulimia and depression. She is afraid that her potential new employer may find out about this and consequently not hire her.
Freedom-related privacy risk	... a loss of freedom of opinion and behaviour may arise from access to his/her information.	An individual believes that entering a sensitive search term into a Web search engine may influence his chance to get a travel permit for a specific country.

not suitable to represent the company or are not loyal to the company. Lastly, *freedom-related privacy risks* refer to individuals being afraid that personal information might be misused to restrict an individual's opinion or behaviour. For example, individuals might be afraid of their decision-making process being influenced by being presented only selected information that aligns with other party's objective: this may be the case when companies try to influence consumers' purchasing decisions by anticipating their preferences and only displaying a limited, tailored set of products. Another example is being restricted in the options that are made available to individuals based on knowledge about them, for example, in terms of insurance services not being offered to individuals with a specific medical history. As with the other dimensions, the probability that individuals assume for these consequences and their severity determines the freedom-related privacy risks dimension. Table 2 lists all seven dimensions and gives a definition and example of each. These privacy risk dimensions in turn form the basis for our scale development.

In contrast to constructs such as general privacy dispositions (Y. Li, 2014), privacy risks involve an individual's perception of the extent to which negative outcomes may arise out of a specific situation in which others may gain access to his or her personal information. Thus, we expect privacy risks to naturally differ across individuals and contexts. We explore this aspect in more depth in Step 5, in the empirical validation of our scale.

3.2 | Step 2: Development of measures

To develop a measurement instrument for multidimensional privacy risks, two steps are necessary (MacKenzie et al., 2011). First, potential items must be generated. Second, the content validity of these items must be assessed to ensure their suitability.

3.2.1 | Item generation

The aim of this step was to create a set of items that fully captures the essence of the focal construct while preventing the items from also touching upon concepts outside the domain of the focal construct (MacKenzie et al., 2011).

For item generation, wherever possible, we relied on existing risk scales (Featherman & Pavlou, 2003; Krasnova et al., 2010; Luo et al., 2010; Stone & Grønhaug, 1993) developed for other contexts. As Karwatzki, Trenz, et al.'s (2017) work informed the conceptualisation of our seven risk dimensions, we also relied on their qualitative dataset, consisting of 22 focus groups with 119 participants to generate suitable items. We developed a variety of items to test which of them best captures the nature of the construct. Overall, we came up with 70 items that could be allocated to the seven dimensions. The initial item set is presented in Appendix C (Supporting information).

3.2.2 | Assessment of content validity

Content validity can be defined as '*the degree to which items in an instrument reflect the content universe to which the instrument will be generalized*' (Straub et al., 2004, p. 424).

To assess the content validity of our items, we used two techniques. First, we performed an open sorting with 10 raters, based on the guidelines of Moore and Benbasat (1991). All raters were carefully selected in order to ensure that they were capable of effectively performing the sorting task and that they corresponded to the main population of interest (MacKenzie et al., 2011), that is, that they were representative of individuals who were likely to encounter the issues queried by our survey. The raters received a number of index cards, each containing a survey item. They were instructed to categorise the items and to label and explain the identified groups. After sorting the items, we asked the raters to discuss any difficulties they encountered with the wording or comprehensibility of the items, and based on the raters' feedback, we dropped some items and adjusted other items.

Second, we applied the rating procedure suggested by Hinkin and Tracey (1999) and recommended by MacKenzie et al. (2011). For this purpose, we selected 20 raters who were representative of our main population of interest and provided them with the definitions of the constructs and the refined items in randomised order. We then asked them to rate the extent to which each item belonged to each construct domain using a 5-point Likert scale. Based on these item ratings, we were able to assess the content adequacy of each item (MacKenzie et al., 2011) by conducting a one-way repeated-measures analysis of variance (ANOVA) for each item.

Our results demonstrated that our raters associated the majority of items with their intended dimensions but indicated that some items were also associated with more than one dimension. The assignment of items to more than one dimension was particularly common for several items belonging to our newly developed dimensions of freedom-related, prosecution-related, career-related and psychological privacy risks. These results, in combination with qualitative feedback from our raters, gave us an indication of which items needed to be reworded or removed.

We then repeated Hinkin and Tracey's (1999) rating procedure to assess the content validity of all adapted and newly added items and presented the rating matrix to 20 new raters. Following this, only a few items – mostly belonging to the freedom-related privacy risk dimension – were again assigned to more than one dimension. Although removing all these ambiguous items would have left us with an item set of an adequate size, we were

curious about the reasons and discussed them with our raters. Based on their feedback, we made some final adjustments to our item set. Appendix D (Supporting information) depicts the item set after this second step of the scale development process.

3.3 | Step 3: Model specification

In this step, we formally specified the measurement model. This specification necessitated defining the relationship between the indicators and their respective privacy risk dimension (first-order level of abstraction) and between the dimensions and overall privacy risk (second-order level of abstraction) (MacKenzie et al., 2011; Wright et al., 2012).

Our model uses seven first-order constructs – namely, our seven privacy risk dimensions: physical, social, resource-related, psychological, prosecution-related, career-related and freedom-related privacy risks. The indicators of every first-order construct are manifestations of the construct, which means that changes in the construct cause changes in the indicators and not vice versa. The indicators of each risk dimension also share a common theme and can be used interchangeably. Finally, we predicted that the indicators of each risk dimension would co-vary with one another and would have the same antecedents and consequences in a nomological network. Thus, we employed a reflective measurement model for each of our privacy risk dimensions (Jarvis et al., 2003).

The second-order level of abstraction – which describes the relationship between the overall privacy risk construct and the different risk dimensions – can be conceptualised as either superordinate or aggregate (Wright et al., 2012). A construct is termed superordinate if the relationship flows from the construct to the dimensions and if the construct is manifested in the dimensions (Wright et al., 2012). However, in our case, the risk dimensions are conceptually different and cover separate aspects of the overall privacy risk construct. The privacy risk dimensions thus define the overall construct in combination, and the flow of relationship is from the risk dimensions to the overall privacy risk construct. These considerations indicate that our model is an aggregate second-order construct. Therefore, we model privacy risks as a reflective first-order, aggregate second-order construct.

3.4 | Step 4: Scale evaluation and refinement

This fourth step of the scale development process aims at a first examination of the properties of the scale, scale refinement and item purification (MacKenzie et al., 2011). We begin by explaining our recruiting procedure and our context of three different apps. Then, we explain the two pretests we conducted to examine the properties of the scale and to refine the measurement items.

All our studies were conducted using Amazon Mechanical Turk (MTurk). A variety of studies have demonstrated the high reliability and quality of data derived from MTurk respondents (Behrend et al., 2011; Buhrmester et al., 2011; Goodman & Paolacci, 2017; Hulland & Miller, 2018; Steelman et al., 2014), making it a suitable alternative to traditional consumer panels. Using a crowdsourcing platform for recruiting our sample seems particularly appropriate in our study because it investigates participants with diverse cognition (Goodman & Paolacci, 2017; Jia et al., 2017). In addition, MTurk is a useful platform to reach individuals who are familiar with the internet and digital technologies. These individuals are potential adopters of innovative digital services, such as the ones we use in the different scenarios of our studies.

Our recruiting procedures and screening techniques followed the recommendations for crowdsourcing platforms (Jia et al., 2017). To avoid potential biases (e.g., lack of attentiveness, lack of ability, self-selection, social desirability and non-independence of participants), we applied procedural remedies that included attention checks, comprehension checks, a moderate compensation, explanations highlighting the importance of the study, neutral wording, no exclusion through filtering, a warning that inattentive respondents will not be paid, quality control, ID comparison and a large sample for the main studies (Hulland & Miller, 2018; Jia et al., 2017; Lowry et al., 2016). To ensure high

TABLE 3 Privacy risk construct with its first-order dimensions and their final items

Dimension	ID	Item
		If someone has access to the information this app has about me…
Physical privacy risk	PH1	… my physical safety might be impacted.
	PH2	… I might be exposed to physical threats.
	PH3	… the chance of me being physically harmed will be increased.
	PH4	… it might endanger my physical safety.
Social privacy risk	SO1	… it might impact the perception that others have of me.
	SO2	… it might change the way people think about me.
	SO3	… my social status might be influenced.
	SO4	… my peer group might think differently of me.
Resource-related privacy risk	RE1	… it might consume my time or my money.
	RE2	… it might cost me time or money.
	RE3	… it might require efforts or expenditures.
	RE4	… it might affect my resources (e.g., time, money) negatively.
Psychological privacy risk	PS1	… it might give me a feeling of anxiety.
	PS2	… it might cause inner restlessness.
	PS3	… I might experience mental tension.
	PS4	… it might burden me mentally.
Prosecution-related privacy risk	PR1	… I might become judicially indictable, either wrongly or rightfully.
	PR2	… I might be prosecuted due to wrongful or rightful suspicions.
	PR3	… I might be held legally accountable due to incorrect or correct suspicions.
	PR4	… I might be held responsible due to incorrect or correct suspicions.
Career-related privacy risks	CR1	… it might reduce my career prospects.
	CR2	… it might affect my career negatively.
	CR3	… it might make it difficult to be successful in my job.
	CR4	… it might result in a negative shift in my career.
Freedom-related privacy risk	FR1	… my opinions or behaviour might be manipulated.
	FR2	… my thoughts or actions might be influenced externally.
	FR3	… my mindset or my resulting behaviour might be influenced.
	FR4	… my attitude or behaviour might be influenced.

data quality, we furthermore restricted participation to users with high reputation scores (at least a 98% approval rating and at least 500 conducted tasks). Additionally, to mitigate cultural biases and minimise the participation of non-native English speakers, we restricted access of our survey to U.S. participants (as suggested by Jia et al., 2017; Peer et al., 2014; Sheehan & Pittman, 2016).

We used the context of different apps for our studies. To select apps that would trigger differences in privacy risk perceptions while still being potentially useful for a broader population, we first identified multiple app candidates drawing on the examples by Karwatzki, Trenz, et al. (2017). We then purposefully designed the app descriptions such that they differed in three aspects: (1) the information they asked the individuals to share; (2) the purpose the information would be used for and (3) the parties that would get access to the information. A qualitative evaluation with five raters allowed us to narrow down the selection to three apps: a health app, a job app and a magazine app. All app descriptions were further fine-tuned through qualitative feedback obtained during the pretests. Detailed

descriptions of the apps are available in Appendix E (Supporting information). To make our cover story as realistic as possible, we told all participants that the study was being performed in cooperation with a start-up company seeking market insights before launching their new app. As a side product, our pretest yielded qualitative and quantitative feedback that confirmed the realism of the developed app descriptions.

Pretest 1 had three aims: (1) to test the comprehensibility of the items and of different alternative scenarios that we planned to use; (2) to perform preliminary reliability and validity assessments and (3) to shorten our instrument. For the first pretest, we collected 61 completed questionnaires in which we measured the items for privacy risk dimensions on a 7-point Likert scale ranging from strongly disagree to strongly agree (as depicted in Appendix F, Supporting information). The questionnaire was preceded by a specific app description such that privacy risks could be evaluated. Appendix F (Supporting information) details the conduct of the pretest, descriptives and analyses. Our results suggest that there was only one overlap among the dimensions; this was due to a few items that we investigated further and finally eliminated. The pretest also provided a first indication of reliability of the scale and triggered minor adaptations to four items. Considering our scales were first applied in this pretest, and the sample was also rather small, we decided to be conservative in shortening our instrument. Based on both quantitative criteria and open text feedback from participants (DeVellis, 2003; Little et al., 1999), we retained five items per risk dimension at this stage.

The aim of Pretest 2 was to reassess the reliability and validity of our shortened measurement instrument with new data in a larger-scale survey and to thereby further refine our instrument. Pretest 2 was administered similar to Pretest 1. Our results from data by 128 participants indicated that the scale was highly reliable with no problematic unintended cross-loadings and thus verified our seven-dimensional conceptual model. Details on the conduct of pretest 2 and the exact values and descriptive statistics for all items can be found in Appendix G (Supporting information). In the process of further shortening the instrument, we decided to retain four items per construct to offer a trade-off between the parsimony of our measurement model and an optimal representation of each construct. We applied the same criteria for shortening as in the first pretest. The final item set, which we validated in the studies described below, is depicted in Table 3.

3.5 | Step 5: Scale validation

After conducting the two pretests and refining the item set in Step 4, Step 5 aimed at re-examining the scale properties and assessing the scale validity with the help of two new samples. We conducted two additional empirical studies (Study 1 and Study 2), which allowed us to do the following: (1) examine our multidimensional privacy risk construct by reassessing the factor structure of the first-order dimensions and by validating the second-order structure; (2) evaluate whether our construct is distinguishable from other constructs and thus exhibits discriminant validity; (3) assess the nomological validity by testing how our construct is related to other constructs and (4) investigate whether our construct is an accurate representation of the underlying construct through experimental manipulation. The last, often neglected, aspect is particularly important because it demonstrates the veridicality of a measurement instrument (i.e., whether the instrument measures what it actually should measure) (Hoehle & Venkatesh, 2015; MacKenzie et al., 2011).

For Study 1, we embedded our privacy risk construct in a nomological network of antecedents and behavioural outcomes (as suggested by Bagozzi, 1980; Edwards, 2001; MacKenzie et al., 2011). Study 1 leverages the three different apps that differ in terms of design and specific risk perceptions – differences that our instrument should be able to clearly identify. Therefore, Study 1 validates our scales and reveals that risk perceptions differ across contexts, making a differentiated view on privacy risk dimensions important and valuable. Study 2 comprises a second experiment that shows that specific privacy risk dimensions within the same context can be influenced by management actions – a finding that goes beyond scale validation as it contributes to privacy research and is also likely to be of much interest to practitioners.

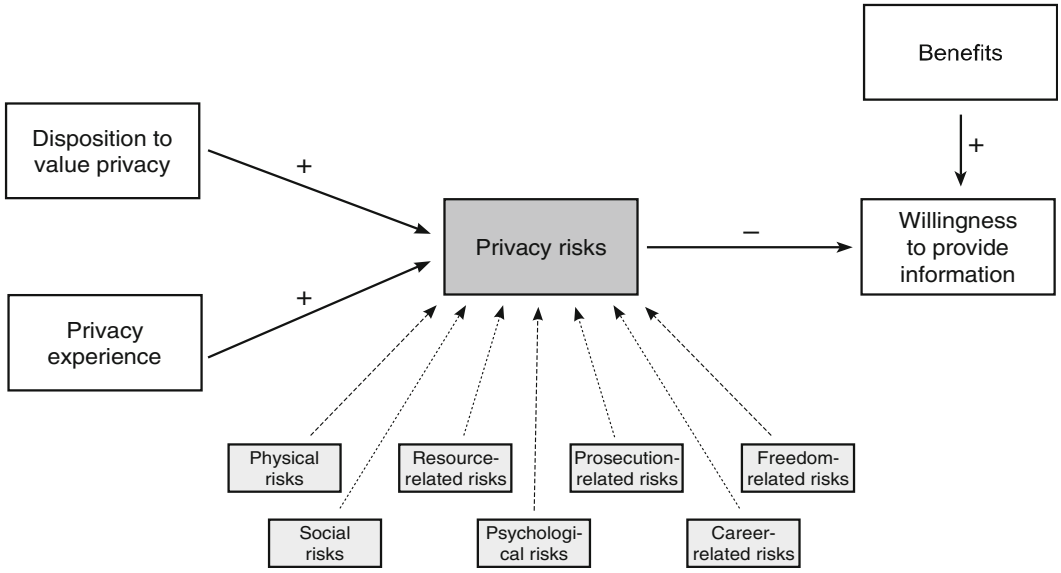

FIGURE 2 Nomological network of validation study

3.5.1 | Study 1: Multidimensional privacy risks in their nomological network and contextual differences

Specification of the nomological network based on the privacy calculus

Evaluating newly developed scales in a nomological network is a critical step in the scale validation process (Hoehle et al., 2016). As recommended by MacKenzie et al. (2011), we selected a nomological network that includes other constructs that are expected to serve as antecedents and consequences of the focal construct. In our context, we drew upon the well-established privacy calculus perspective, which assumes that individuals perform a risk–benefit analysis when deciding whether and how much personal information to disclose to other parties (Culnan & Bies, 2003; Dinev & Hart, 2006; Smith et al., 2011). Using this abstraction of the underlying decision-making process, previous studies have shown that it is a fruitful perspective that helps better understand individuals' information disclosure behaviour when facing privacy-intrusive situations (Dinev & Hart, 2006; Kehr et al., 2015; Krasnova et al., 2010).

In line with prior privacy research (Bélanger & Crossler, 2011; Smith et al., 2011), we decided to use *willingness to provide information to an app* as a dependent variable in our nomological network. Out of the wide variety of potential predictors of privacy perceptions, *privacy experiences* and personality differences such as individuals' *disposition to value privacy* constitute situation-independent, privacy specific drivers of privacy perceptions (Smith et al., 2011).

We integrated these two types of antecedents in our nomological network due to their cross-situational applicability. Privacy experiences refer to an individual's prior negative experiences associated with being exposed to or being victimised by information abuse (Y. Li, 2014; Smith et al., 1996). We anticipated that privacy experiences would have a positive influence on our privacy risk construct. An individual's disposition to value privacy refers to a person's general attitude toward privacy and has been shown to positively influence other privacy constructs (Y. Li, 2014). To measure these antecedents and the outcome variable, we relied on validated scales (see Appendix H, Supporting information). Figure 2 depicts the nomological network that we used to validate our privacy risk construct.

Contextual differences in the importance of privacy risk dimensions

Based on our assumption that the impact of the seven risk dimensions varies across contexts, we anticipated that the average assessment of each risk dimension would differ across situations. Identifying these differences would allow us to better address context-specific privacy risks and thus make a multidimensional conceptualisation of privacy risks more useful. As these privacy risk dimensions could not be assessed prior to the development of our measurement instrument, we drew on our theoretical framework of the risk dimensions and the underlying adverse consequences to contrast contexts where we expect certain privacy risk dimensions to be more and less prevalent. Such differences in privacy risk dimensions can be explained by differing personal information sharing requirements or by the different parties that may get access to the personal information.

We, therefore, leveraged our three apps (health, job, magazine) that were purposefully developed to exhibit such differences in sharing requirements and parties with access. The examples by prior studies touching upon privacy-related adverse consequences suggest that job and health may be associated with very specific adverse consequences (i.e., career- and freedom-related respectively), while the adverse consequences arising from a magazine app are less predetermined by those contextual characteristics. We therefore briefly elaborate on those aspects and formulate two testable expectations below that can help to verify the ability of our scale to assess such differences.

First, career-related privacy risks occur when individuals fear that access to personal information may negatively influence their career. The job app (see Appendix E, Supporting information) is intended to help users find a new job through a portal providing individualised job suggestions based on users' backgrounds and preferences. This app simplifies the job application process by allowing users to easily share documents such as certificates or references with companies. In this job app, users were encouraged to not only share details about their resumes and job preferences but also about what they like and dislike about their current jobs and what they desire. Such information is highly sensitive and could lead to negative consequences if unintended parties were to obtain access to it (Karwatzki, Trenz, et al., 2017; Schmoll & Bader, 2019). In particular, current (or future) employers' access to this information may significantly hinder employees' career in the future. For example, true preferences that are required for effective matching (e.g., the search for a relaxed job) may not be evaluated favourably, the employer may assume that an individual is not suitable to represent the company, or there could be a biased evaluation through algorithms (Ghosh, 2017; Moise, 2018; Raghavan et al., 2020). In contrast, the information required to be shared with the magazine app (e.g., interests, GPS) is equally sensitive but not of primary interest for making career-relevant decisions. As we set out to confirm that our measurement scale would be able to reflect such contextual differences on a risk dimension-level, we contrast the job app to the magazine app, and expect that the career-related risk dimension is more prevalent in the job app context than in the magazine app context (*hypothesis 1*).

Second, freedom-related risks are frequently linked to settings where individuals may be discriminated against based on their status – for instance, their health status (Karwatzki, Trenz, et al., 2017). The health app (see Appendix E, Supporting information) tracks information – such as activities, nutrition, sleeping behaviour and body measure – that could be shared with insurance companies. Such self-surveillance technologies were found to not only empower but also disempower individuals (De Moya & Pallud, 2020). If available to third parties, the data collected by this app may be used to restrict individuals' options to a limited, tailored set of services or by exploiting their characteristics to manipulate their decisions. Fears of being discriminated against based on their health status should be particularly strong in this context. We again used the magazine app as a comparative setting to identify contextual differences and expect that the freedom-related risk dimension is more pronounced in the health app than in the magazine app context (*hypothesis 2*).

It is important to note that while these differences are grounded in the theoretical pre-understanding that led to the apps investigated, other differences may emerge throughout the evaluation. As such, the measurement instrument may (and should) be used to explore differences in settings where a theoretical pre-understanding is lacking – exploiting the opportunities for expanding our existing knowledge on information privacy that arise with the availability of the new scale.

Study conduct and sample description

We administered the questionnaire for Study 1 as follows. To ensure that participants could assess their privacy experience and their disposition to value privacy without having a specific context in mind, we first assessed these two antecedents of our nomological network. We then randomly assigned participants to one of the three apps (magazine app, job app, health app). After reading the respective app descriptions, participants were asked for their assessment, which included measuring their willingness to give the app access to their personal information, our dependent variable. Following this, participants assessed their perceptions of the privacy risks and benefits of the service. Finally, we measured a marker variable, participants answered a few control questions, and the survey concluded with questions on demographic details and a debriefing.

Our survey design paid special attention to detecting and attempting to prevent the satisficing behaviour of participants, which is a major concern for survey research (Krosnick, 1991). We applied several measures. First, following the recommendations of Jia et al. (2017), we informed participants at the beginning that their answers were crucial for our study and that they would not be paid if they failed to answer questions carefully. Having survey work rejected has negative implications for MTurk participants because it reduces their chances of getting work in the future. Second, we told participants that our research was conducted in cooperation with a start-up company that was interested in evaluating the potential of its new app, thereby hoping that participants would provide thoughtful and truthful answers in order to help the start-up team. We also included an instructional manipulation check that instructed participants to click on a headline instead of on the 'next' button to continue the survey (Oppenheimer et al., 2009). Furthermore, to detect and eliminate participants who did not contribute any valuable answers, we included a few risk items twice on subsequent pages and looked at deviations. We also took the overall response time into consideration and deleted respondents who finished the survey in less than half the average time.

We conducted our survey on MTurk and obtained a total of 662 valid responses. Participants' age varied between 18 and 74 years (with a mean age of 34 years and a standard deviation of 19.38), and 56.6% of the participants were female. Additionally, 33.3% of the participants reported a yearly household income below $35 000, 43.5% between $35 000 and $75 000, and the remaining 23.2% more than $75 000 per year. Thus, our sample represented a broad cross-section of the US population and was not biased towards a specific age group, gender or income group.

Data evaluation and results

As a first step in analysing the data, we repeated the factor analysis conducted in Pretest 2. Again, the pattern matrix revealed the expected seven factors with unique loadings of each item on the expected factor. The structure matrix showed high correlations for the expected relationships between the items and factors (all well above 0.8) and low correlations (all well below 0.7) between the items and factors to which they should not have been linked.

We then needed to further examine our measurement model and to assess privacy risks in the nomological network. To evaluate our nomological model, we used Smart PLS for three reasons (see Hair et al., 2017): the exploratory character of the study; the primary interest of identifying potential relationships between variables (Hair et al., 2016; Hair et al., 2018); and the underlying philosophy of measurement, which is a composite factor model that supports the modelling of our second-order aggregate constructs (Carter et al., 2014; Karimi & Walter, 2015; I. Walsh et al., 2016).

We applied a repeated indicators approach to model our first-order reflective, second-order aggregate privacy risk construct (Hair et al., 2018). To evaluate the measurement model, we first assessed the validity and reliability of the first-order constructs of privacy risks and all other constructs of the nomological network. All our constructs exhibited Cronbach's alpha and composite reliability above the recommended threshold of 0.7 (Fornell & Larcker, 1981; Nunnally & Bernstein, 1994). All factor loadings were above 0.708, indicating convergent validity. At the construct level, average variance extracted exceeded 0.7 for all risk constructs and was thus larger than the threshold of 0.5 (MacKenzie et al., 2011). We also assessed discriminant validity by using the Fornell–Larcker criterion (Fornell & Larcker, 1981), which was also fulfilled. Moreover, we assessed the Heterotrait–Monotrait ratio of all

correlations and found them to be well below the conservative threshold of 0.85 (Hair et al., 2018). We can thus conclude that our sample had an adequate level of discriminant validity. Detailed statistics are reported in Appendix I (Supporting information).

To assess the measurement model of our second-order privacy risk construct, we assessed the weights between the first-order risk dimensions and overall privacy risk (Hair et al., 2018). The analysis shows that all risk dimensions significantly influence the second-order construct and that the effects are similar in size: physical privacy risks, $\beta = 0.17$, $p < 0.001$; social privacy risks, $\beta = 0.20$, $p < 0.001$; resource-related privacy risks, $\beta = 0.20$, $p < 0.001$; psychological privacy risks, $\beta = 0.21$, $p < 0.001$; prosecution-related privacy risks, $\beta = 0.20$, $p < 0.001$; career-related privacy risks, $\beta = 0.22$, $p < 0.001$ and freedom-related privacy risks, $\beta = 0.20$, $p < 0.001$. We checked for potential collinearity between the first-order risk constructs and the variance inflation factors (VIF) of all risk dimensions are well below the conservative threshold of 3.33 (Diamantopoulos & Siguaw, 2006).

We applied multiple approaches to prevent and identify potential common method bias. Details on these approaches and post-hoc tests can be found in Appendix J (Supporting information). In summary, the results showed that common method bias is not prevalent in our dataset.

The results of the analysis of our nomological network are presented in Figure 3. We found a negative impact of privacy risks ($\beta = -0.19$, $p < 0.001$) on users' willingness to disclose information to the app after controlling for the influence of benefits ($\beta = 0.62$, $p < 0.001$). To investigate the influence of the antecedents on a higher-order construct (which was modelled via the repeated indicators approach), a total-effects analysis must be applied (Hair et al., 2018). This analysis reveals significant influences of individuals' disposition to value privacy ($\beta = 0.15$, $p < 0.001$) and privacy experiences ($\beta = 0.14$, $p < 0.001$) on privacy risks. We also controlled for demographics such as age, gender and income. The analysis resulted in only insignificant relationships, and all control variables were thus excluded from the final model. Overall, the research model explains 42% of individuals' willingness to disclose information. Because we found support for all relationships between our focal construct privacy risks and its antecedents and outcome, we can conclude that nomological validity is present.

Another aim of Study 1 was to demonstrate that our privacy risk scales adequately represented the underlying risk construct. Based on the recommendations of MacKenzie et al. (2011), we designed this study to experimentally manipulate the privacy risk construct – in particular, its dimensions – by exposing our participants to different app descriptions. We anticipated that the three apps – job app, health app and magazine app – would affect individuals' assessment of the risk dimensions differently. Because we used a between-subject design with multiple dependent variables (namely, all the privacy risk dimensions), we selected a multivariate analysis of variance (MANOVA) as a method of choice to investigate whether individuals' risk assessment differed across the three apps.[2]

To use our privacy risk dimensions as dependent variables in the MANOVA, we derived factor scores using the regression method. The MANOVA shows that there are significant differences across the three apps (Pillai's Trace = 0.23; $F(14,1308) = 12.12$, $p < 0.001$). As follow-up tests, we conducted a series of one-way ANOVAs on each of the seven risk dimensions. These indicated significant differences for career-related privacy risks ($F(2,659) = 42.63$, $p < 0.001$), freedom-related privacy risks ($F(2,659) = 3.26$, $p < 0.05$), physical privacy risks ($F(2,659) = 4.35$, $p < 0.05$) and prosecution-related privacy risks ($F(2,659) = 3.63$, $p < 0.05$). There were no significant differences for psychological privacy risks ($F(2,659) = 2.02$, $p > 0.05$), resource-related privacy risks ($F(2,659) = 0.04$, $p > 0.05$) or social privacy risks ($F(2,659) = 2.74$, $p > 0.05$).

To further investigate the significant mean differences across the three apps, we performed a series of post hoc analyses (with the conservative Bonferroni correction to account for potential type I error inflation). As expected and outlined in hypothesis 1, career-related risks were higher in the job app than in the magazine app (mean difference = 0.62, $p < 0.001$). It was also higher in the job app compared to the health app (mean difference = 0.78, $p < 0.001$). As suggested in hypothesis 2, freedom-related risks were significantly higher in the health app than in the magazine app (mean difference = 0.28, $p < 0.05$). Beyond those proposed results, we found further differences in physical privacy risks (mean difference = 0.62, $p < 0.001$) and prosecution-related privacy risks (mean difference = 0.24, $p < 0.001$), which were both higher in the health app than in the job app. We speculate that these

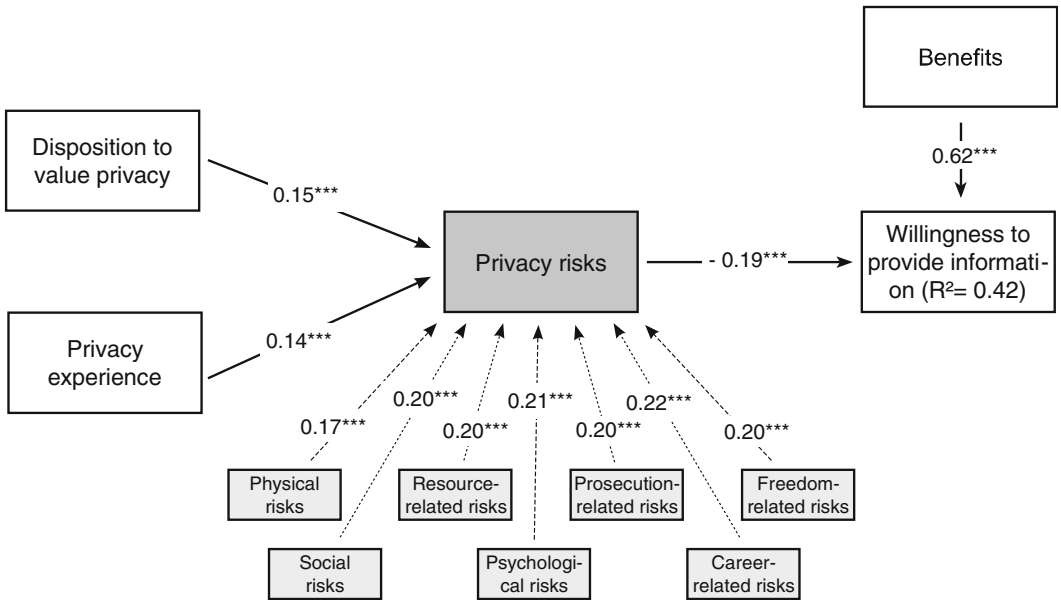

FIGURE 3 PLS structural results. *$p < 0.05$, **$p < 0.01$, ***$p < 0.001$

differences may be due to the health app's continuous tracking of GPS data, which is shared with a community of other health app users. Individuals may fear that other people could misuse their information, for example, to physically harm them or arouse suspicions implicating them in some type of wrongdoing (Karwatzki, Trenz, et al., 2017). All other comparisons yielded insignificant results.

Summary

Study 1 demonstrated the reliability and validity of our newly developed measurement instrument; testing privacy risks in a nomological network indicates the instrument's usefulness. Moreover, the dimensions of the privacy risk construct varied across contexts as expected, providing further evidence that our measurement instrument actually measures what it is intended to. Lastly, the results of Study 1 uncover further variations of privacy dimensions between contexts that could not be predicted based on the existing pre-understanding of the nature of privacy risks. Thereby, the results give a first indication of how our fine-grained perspective on privacy risks will facilitate a richer and deeper understanding of contextual differences.

3.5.2 | Study 2: Targeted mitigation of privacy risk dimensions through technology or service design

While in Study 1, we looked at how the level of privacy risk differed across contexts, in Study 2, we investigate whether we can manipulate the level of certain types of privacy risks in a targeted fashion. The ability to influence specific dimensions of the multidimensional privacy risk concept would further emphasise the importance of the fine-grained level of investigation enabled by our new scales. This study thus goes beyond pure scale validation; it exemplarily demonstrates the concrete application of the scales to inform technology design.

Mitigating privacy risk dimensions

A number of studies have been conducted to investigate how information systems design can influence privacy on an aggregate level (Hu et al., 2010; Hui et al., 2007; Sutanto et al., 2013; H. Xu et al., 2009). Two common design elements are the use of privacy dashboards and trusted intermediaries. Privacy dashboards have played a major role, providing individuals with information and control over their data and its usage (Karwatzki, Dytynko, et al., 2017; Krasnova et al., 2010). Another tool to give users more control is to prevent an untrusted firm's access to the data in the first place, for instance by involving trusted intermediaries. Such intermediaries could handle parts of the transaction process such as the payment (Giaglis et al., 2002). We selected these two established mitigators because they would definitely decrease privacy risks on a general level. However, our goal was to identify whether we could use such design elements to target selected dimensions of privacy risks. The payment intermediary and the privacy dashboard were particularly suitable because the first specifically aims at the payment process and the resources of the users, while the other is more general, giving more information control to the user.

Prior studies have already shown the effectiveness of trusted intermediaries in an e-commerce context (Verhagen et al., 2006), focussing on transaction rather than privacy risks. Building upon this stream of research, we predicted that the partnership with a trusted and well-known party that facilitates the payment process would lead to reduced resource-related privacy risk perceptions (*hypothesis 3*).

We anticipated that a privacy dashboard that allows individuals to see and control what information was collected and what it was used for would reduce individuals' privacy risks. While there is a common understanding that control will influence privacy perceptions in general (Karwatzki, Dytynko, et al., 2017; Krasnova et al., 2010), the lack of a multidimensional privacy risk conceptualisation prevented prior studies from deriving insights into which particular privacy risk dimensions may be mitigated by a specific control mechanism. We, therefore, build upon our insights on privacy-related adverse consequences and the rich examples (provided by the sources in Table 1) to derive testable expectations.

In particular, we expected that individual control via a privacy dashboard would mitigate privacy risks along four different privacy risk dimensions. First, we expected to observe lower freedom-related privacy risks (*hypothesis 4a*) because participants could prevent their information from being used for selected purposes (such as advertising) or being shared with third parties (such as insurance companies). Second, we expected that participants using privacy dashboards would exhibit lower physical privacy risks (*hypothesis 4b*) and prosecution-related privacy risks (*hypothesis 4c*) because they could better control whether information (such as GPS data) was collected and thereby subject to potential misuse. Finally, we expected that participants would experience lower social privacy risks (*hypothesis 4d*) because they could decide what information was shared with the community.

Study conduct and sample description

Study 2 used again the health app. We designed two manipulations extending the health app in ways that we expected would mitigate specific risk dimensions: (1) a privacy dashboard and (2) a payment partnership between the app provider and PayPal. In the first manipulation (privacy dashboard), participants were informed that the dashboard was intended to give app users more control over their information by allowing them to specify what information was automatically delivered to the app, for what purposes, and who could gain access to which information. In the second manipulation (the payment partnership), the health app informed participants that all payments (i.e., the monthly app subscription) could be made through PayPal so that disclosing financial information was unnecessary. Details on both manipulations can be found in Appendix L (Supporting information).

During the experiment, we first primed participants to be sensitive to privacy issues by asking them to read a news article about a recent privacy incident and to answer several questions about it. Otherwise, by first triggering this awareness through the term 'privacy issues', our manipulations could have had unintended side effects that diminished the true effect of the manipulations. We then randomly assigned the participants to one of the three groups: one of the two treatment groups or to the control group. Participants in the two treatment groups were shown a description of the health app combined with one of the risk mitigation manipulations (either privacy

dashboard or payment partnership), while participants in the control group were exposed to the same description of the health app without any additional manipulation. Participants were then asked to assess their privacy risk perceptions, which was followed by a manipulation check. Finally, demographic details were collected, and participants were debriefed. To prevent and detect satisficing behaviour among participants, we applied the same measures as those used in Study 1.

We collected 185 valid responses in Study 2. Our participants were between 20 and 72 years old (with an average of 38.29 years and a standard deviation of 11.35), and 56.8% of our participants were female. Additionally, 37.8% of the participants reported a yearly household income below $35 000, 45.9% between $35 000 and $75 000, and the remaining 27% above $75 000. Thus, once again, the sample obtained via MTurk reflected no strong bias toward any specific demographic class.

Data evaluation and results

Before analysing the data, we performed a manipulation check. At the end of the survey, we included two manipulation check items to ensure that participants correctly recalled which app they were presented with – and indeed all the participants did so.

As in Study 1, MANOVA was the preferred analysis method in Study 2 for investigating whether the two manipulations triggered a change in participants' risk assessment. We derived factor scores based on the regression method to use all risk dimensions as dependent variables in the MANOVA. We found significant differences between the three groups (Pillai's Trace = 0.13; $F(14,354) = 1.725$, $p < 0.05$).

To further investigate these differences, we conducted a series of one-way ANOVAs on each of the seven risk dimensions. These indicated significant differences for freedom-related privacy risks ($F(2,182) = 4.68$, $p < 0.05$), physical privacy risks ($F(2,182) = 4.33$, $p < 0.05$), prosecution-related privacy risks ($F(2,182) = 3.59$, $p < 0.05$), psychological privacy risks ($F(2,182) = 3.97$, $p < 0.05$), resource-related privacy risks ($F(2,182) = 4.30$, $p < 0.05$), and social privacy risks ($F(2,182) = 4.75$, $p < 0.05$), but no significant differences for career-related privacy risks ($F(2,182) = 2.04$, $p > 0.05$).

To follow up on the significant mean differences between the groups, we performed a series of post hoc analyses (with the conservative Bonferroni correction). As expected, we found that the partnership between the app provider and PayPal significantly mitigated resource-related privacy risks (mean difference = −0.48, $p < 0.05$; hypothesis 3). Interestingly, psychological privacy risks were also significantly lower in the PayPal treatment group than in the control group (mean difference = −0.50, $p < 0.05$). A possible explanation for this unintended finding is that trust may have been transferred from PayPal to the app provider, which was an unknown start-up company, thereby exerting a positive influence on participants' peace of mind. Such a trust transferal has also been observed in other studies (Delgado-Márquez et al., 2012; Jiang et al., 2008; Lowry et al., 2008). The PayPal partnership did not significantly reduce any other risk perceptions.

Regarding the treatment group with the privacy dashboard, our expectations were also confirmed. Freedom-related privacy risks (mean difference = −0.51, $p < 0.05$), physical privacy risks (mean difference = −0.47, $p < 0.05$), prosecution-related privacy risks (mean difference = −0.47, $p < 0.05$) and social privacy risks (mean difference = −0.54, $p < 0.05$) were significantly lower in the privacy dashboard treatment group than in the control group (hypotheses 4a-d), while the means of all other risk dimensions did not differ significantly.

Summary

These results provide further evidence of the necessity and value of our multidimensional conceptualisation of privacy risks. We were able to show that the perceptions of privacy risk dimensions differ within and between contexts and that they can be actively influenced by design decisions. These findings thus go beyond demonstrating the validity of our scales; they also have major theoretical and practical implications, which we discuss in the following section.

4 | DISCUSSION AND IMPLICATIONS

Our study had two aims: to develop a multidimensional conceptualisation of privacy risks that captures the different negative outcomes that individuals may fear when other parties access their information and to explore the advantages of a fine-grained perspective on privacy risks. Our conceptualisation of privacy risks consists of seven privacy risk dimensions: physical, social, resource-related, psychological, prosecution-related, career-related and freedom-related. Based on several steps of qualitative and quantitative assessment of data from over 1000 participants, we developed a measurement instrument to account for these different dimensions and demonstrated the reliability, validity and usefulness of this instrument. Applying this measurement instrument revealed novel insights concerning the nature of privacy risks and how to mitigate them.

In the following, we outline how our work contributes to theory and practice. Our work also offers promising avenues for further exploration of how privacy perceptions influence individuals' behaviour and how these perceptions can be managed.

4.1 | Implications for theory

Despite the importance of privacy risks in IS research, our literature review revealed that there is a lack of theoretical clarity on the nature of privacy risks and a lack of tools to measure the dimensions of privacy risks to more effectively design digital services. Our work addresses these issues by providing a fine-grained conceptualisation of multidimensional privacy risks, offering a reliable and valid measurement instrument and showcasing the instrument's value. This advances the existing body of knowledge in several ways.

First, we disentangled the previously aggregated concept of privacy risks into its constituting dimensions – namely physical, social, resource-related, psychological, prosecution-related, career-related and freedom-related privacy risks. Privacy risks were established as an important determinant of privacy-related behaviours such as information disclosure, but conceptualisations of privacy risks have so far failed to capture how individuals believe possible negative consequences of information sharing might affect them (Dinev et al., 2006; Dinev & Hart, 2006; Hong & Thong, 2013; Malhotra et al., 2004; Smith et al., 1996). Our rich multidimensional conceptualisation specifies the types of impact that may occur and thus complements prior conceptualisations of privacy risks in a way that is particularly useful if a more precise attribution of the nature of the perceived risks is of interest. Similarly nuanced conceptualisations of risk have proven valuable in domains other than information privacy (Featherman & Pavlou, 2003; Luo et al., 2010). In a similar fashion, being able to distinguish between dimensions of perceived privacy risks opens up avenues for a deeper understanding of privacy and a more granular level of analysis (Polites et al., 2012). The application areas in which an attribution of particular consequences to perceived privacy risks is critical include not only all digital services and digital apps offered by companies but also data-intense broader initiatives such as data donation to facilitate research advances or to mitigate public crises (e.g., pandemics).

Second, we developed and validated a reliable and valid measurement instrument (displayed in Table 3) for capturing this multidimensional conceptualisation. After applying rigorous scale development and validation procedures (MacKenzie et al., 2011), we demonstrated that our measurement scale serves as a reliable and valid tool that researchers can use to assess and understand the nature of privacy risks. In this sense, our multidimensional privacy risk conceptualisation and instrument can both be used as a springboard for future research. In light of greater discourse on digital services, information disclosure, consumer rights, big data and privacy violations, the importance of acquiring fine-grained insights into privacy perceptions is constantly increasing. Our novel perspective on how to measure privacy-related perceptions can offer a theoretical and methodological foundation for further advancements in this field.

For example, recent privacy research has highlighted the importance of multiple levels of privacy because individuals' privacy states and decisions are interdependent (Bélanger & James, 2020). At the same time, privacy

research has focussed on individuals' disclosure of information, while indirect users or those affected on a macro level have not been considered (Leidner & Tona, 2021). As privacy research expands its scope from an interaction between individuals and organisations towards complex interpersonal and interfirm relationships, linking privacy perceptions to specific organisational practices might become challenging. Multidimensional views on privacy (Hong & Thong, 2013; Malhotra et al., 2004; Smith et al., 1996) refer to aspects such as improper access, unauthorised secondary use, errors, collection, control and awareness (Hong & Thong, 2013). However, firms' behaviour (Dinev & Hart, 2006) is only one aspect that may trigger negative consequences in complex environments where personal data is shared across individuals, groups and firms. As our multidimensional privacy risk scale measures the perceived risk levels across dimensions without being restricted by specific causes of those risks, our scale should prove valuable in facilitating empirical discoveries in this – thus far mostly conceptual – research stream (Bélanger & James, 2020; Leidner & Tona, 2021).

Third, our results indicate that the dimensions of privacy risks can vary independently across contexts and are thus not necessarily correlated. Therefore, while an aggregate perspective on privacy risks may have led to comparable risk-level evaluations for different services (Bansal et al., 2010), our study indicates that the nature of these privacy risks can diverge significantly even though the aggregated risk perception levels might be comparable. This may also explain why sharing behaviours of identical information can vary across contexts (H. Li et al., 2010). Our work thereby responds to the call for more contextualised research in information systems and the issue of partiality of theory (Avgerou, 2019) that naturally arises from the tradeoff between scale and detail. In fact, most research on privacy risks has so far aimed at generalisability and parsimony by collapsing privacy risks (e.g., Dinev et al., 2006; Krasnova et al., 2010; Liu et al., 2019; H. Xu et al., 2011). While the value of generalisability is unquestioned (Gregor, 2006; Lee & Baskerville, 2012), disentangling the dimensions of privacy risks has revealed significant contextual differences in privacy risk perceptions. This complementary perspective has the potential to develop richer theories that at the same time provide more actionable advice (Hong et al., 2013; Weber, 2003). As our data-driven world makes privacy phenomena ubiquitous, it is unlikely that established relationships hold across all contexts, ranging from online social networks (Liu et al., 2019), tracing technologies (Trang et al., 2020), personal data marketplaces (Spiekermann et al., 2015), smart devices (Ogbanufe & Gerhart, 2020), to digital platforms (Teubner & Flath, 2019). The concepts and scales developed in our work bear the potential to increase the realism of studies on information privacy (Edwards, 2001) and facilitate a more in-depth understanding of the privacy risks that occur in particular contexts and settings.

Fourth, our findings contribute to literature on privacy design in the sense that they indicate the necessity and possibility of target-oriented mitigation of privacy risk perceptions. While prior studies have suggested that trusted intermediaries or seals are generally valuable options for privacy risk mitigation (Belanger et al., 2002; Faja & Trimi, 2006; H. Xu et al., 2008), our study shows that the effectiveness of those countermeasures is specific to the nature of the privacy risk – that is, the dimensions of privacy risks that are particularly pronounced for certain services. Our findings thus constitute a starting point for developing a more concise account of the relationship between technology design and perceptions of privacy risk (Law et al., 1998). They imply that technology design must directly address those privacy risks that are prominent in its particular context. In this sense, our results provide a first step toward a deeper understanding of whether, why and how risk mitigation mechanisms work; previous studies have only discussed this on a rather abstract or speculative level (Hui et al., 2007; H. Xu et al., 2011).

Lastly, despite the seminal nature of the article by MacKenzie et al. (2011), only a few articles have thus far exercised and documented all of the steps for establishing new measurement instruments. However, ours has done so. In this sense, our work may be helpful to future researchers attempting to develop new measurement instruments and report their results. In particular, we showcase how the often-neglected aspect of veridicality of the measurement instrument can be demonstrated using experimental manipulation (Hoehle & Venkatesh, 2015; MacKenzie et al., 2011). This is particularly important for researchers aiming not only at explanation but also at deriving prescriptive statements on how to design technologies or socio-technical systems (Gregor, 2006). The ability to capture

perceptions of interventions or alternative designs using measurement instruments is paramount to accelerated scientific progress.

4.2 | Implications for practice

Our study has several important implications for practitioners. Many business models – including those related to innovative apps, cloud services and digital platforms – depend on rapid growth rates and on the collection and analysis of user data. Therefore, these service providers are keenly interested in better understanding the circumstances of individual information disclosure, reasons that might prevent disclosure, and how to mitigate problematic influences.

By conceptualising privacy risks as a multidimensional construct and by demonstrating its influence on information disclosure intention, we offer organisations a better understanding of why consumers might hesitate to share information in certain situations and how these privacy risk perceptions are formed. While firms might have a solid understanding of the objective risks that may arise from their service configurations, individuals' perceptions of those risks are not always objective (Gerlach et al., 2019). At the same time, relative changes in privacy risk perceptions are key to influencing actual disclosure decisions (Adjerid et al., 2018), putting perceived risk at their center of attention. We assessed individuals' privacy risk perceptions across three apps that differed in several ways, including the type of information asked for and the involved parties. We showed that our scale for measuring the various risk dimensions can be used to reveal the differences in individuals' assessment of these situations, which should be of great interest to practitioners. Our results on the selected apps already point toward specific privacy risk dimensions that developers should consider. For example, the rising class of health applications requires individuals to share personal data including health-related information and access to sensor data. The general dilemma is that, while unauthorised access to this sensitive information could have many different negative consequences for users, this information is required for providers to offer such digital services. Our results guide developers and suggest that, in this context, developers need to focus their attention on design mechanisms that defuse users' beliefs that their freedom of expression and behaviour may be compromised by this data access. Interestingly, our results also identified privacy-specific differences that came as a surprise at first. For instance, we found that the risk that legal actions may be taken against an individual was more prominent in the health app than in the job app. Such issues are likely not the primary considerations of health application designers but may in fact hinder data sharing and use if not understood and mitigated.

Not only are the results of our study or of future studies using our instrument useful to organisations, but organisations may also use our scale directly for their own purposes. Our instrument could be used by practitioners to study to-be-developed, to-be-implemented, as well as existing digital services that require users to disclose information. It can be used by system developers and service designers to gain insights into which privacy risk dimensions are most prevalent in a specific situation. These insights help organisations understand which risks to best mitigate by the service design and which risk mitigation mechanisms to use to assuage the fears of reluctant users. Following implementation, our measurement instrument can also assess the effectiveness of these mechanisms.

4.3 | Limitations and suggestions for future research

While our nomological network offers a good starting point for investigating the causes and effects of privacy risk, it is far from complete.

In our study, we investigated only a limited number of constructs – namely, individuals' disposition to value privacy, privacy experience and willingness to disclose information. However, many other constructs (antecedents and outcomes) would be worthy of further study. For example, personality-related factors such as openness to

experience and neuroticism have been shown to influence individuals' threat appraisal (Bansal et al., 2010; Junglas et al., 2008). The same applies to cultural factors such as uncertainty avoidance or collectivism (Lowry et al., 2011) and situation-specific variables such as familiarity with a situation or mobile-computing self-efficacy (Keith et al., 2015; Y. Li, 2014). It would thus be interesting to investigate the role of such factors in privacy risk formation.

Regarding outcome variables, we focussed on the well-established construct of willingness to provide information to a service. However, intentions are only a proxy for actual behaviour. Future research could not only leverage our measurement instrument to further elucidate how privacy risks influence behavioural intentions – such as intention to use or to continue to use a service – but could also use the instrument to clarify users' actual behaviour, which remains under-investigated in privacy literature (Dinev et al., 2015; Kokolakis, 2017; Smith et al., 2011).

We investigated privacy risks only in the context of innovative apps. Future research should explore the influence of privacy risks in other contexts as well. Of particular interest are the contexts in which individuals must disclose personal information to access a service – for example, social networking, e-commerce, or any other service that offers personalised content and recommendations. Such research would enable a more fine-grained understanding of how privacy risks influence user behaviour in different settings.

The multidimensional conceptualisation of privacy risks also opens up new research opportunities in terms of how other parties can actively mitigate privacy risks. To demonstrate the usefulness of our scales, we investigated privacy dashboards and partnerships with trusted third parties as risk mitigation mechanisms. There are many more such mitigation mechanisms – such as seals, privacy policies or the development of trust and long-term relationships – whose effect on the multiple dimensions of privacy risk could be evaluated. Knowledge about which risk dimensions are especially prevalent in which situations can additionally inform the design of suitable new risk mitigation mechanisms. This research direction is also of high practical relevance because organisations are increasingly interested in manipulating the privacy risk perceptions of online users so that users' information disclosure behaviours can be better aligned with their own organisational aims.

Similarly, governments have intensified their efforts to collect citizen data to address societal issues such as the COVID-19 pandemic. However, their acceptance is held back by privacy risk beliefs that are difficult to comprehend if you analyse only the technological configuration (Trang et al., 2020). In-depth analysis of those perceptions, as enabled by our multidimensional approach to privacy risk, can therefore help governments design apps that are not feared by citizens and more effectively meet societal needs.

5 | CONCLUSION

This article attempts to fully explicate the nature of privacy risks. We posit that privacy risks is a multidimensional concept and that the lack of understanding of which specific privacy risks are present in which contexts and situations makes it difficult to implement technologies that would mitigate such risks. We therefore first conceptualise multidimensional privacy risks using a taxonomical approach consisting of physical, social, resource-related, psychological, prosecution-related, career-related and freedom-related privacy risks. Building upon a series of qualitative and quantitative studies, we develop and validate a scale that measures multidimensional privacy risks. Then, using both cross-sectional as well as experimental studies, our results showcase how different dimensions of privacy risks are in fact differently pronounced across contexts and how technology designs can be tailored to mitigate them.

From a theoretical perspective, our findings advance research on privacy by disentangling the concept of privacy risks conceptually into its constituting dimensions and by providing a valid and reliable instrument to measure it. At the same time, the results provide initial insights into contextual and service-specific differences in privacy risk dimensions and open up new avenues for researchers trying to contribute to a contextualised and actionable understanding of privacy. From a practical perspective, our results can help managers to understand the nature of privacy risks related to their service and to adjust their digital offerings to mitigate users' privacy risk perceptions.

ENDNOTES

[1] Throughout the remainder of this study, following Smith et al. (2011) and Dinev et al. (2013), the term 'privacy' refers specifically to information privacy.

[2] While few MANOVA assumptions are violated in our sample, several simulation studies have shown that MANOVA is fairly robust (Hair et al., 2014; Howell, 2013). However, to verify our results, we additionally ran a Kruskal–Wallis H-test, which is a rank-based nonparametric test and thus has lower distributional requirements. As can be seen in Appendix K (Supporting information), this test reveals the same differences in the risk dimensions between the three apps, providing further support for our results.

DATA AVAILABILITY STATEMENT

The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

ORCID

Manuel Trenz https://orcid.org/0000-0002-8970-958X
Daniel Veit https://orcid.org/0000-0003-4657-2883

REFERENCES

Abbasi, A., Sarker, S., & Chiang, R. H. (2016). Big data research in information systems: Toward an inclusive research agenda. *Journal of the Association for Information Systems*, *17*(2), i–xxxii. https://doi.org/10.17705/1jais.00423

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509–514. https://doi.org/10.1126/science.aaa1465

Adjerid, I., Peer, E., & Acquisti, A. (2018). Beyond the privacy paradox: Objective versus relative risk in privacy decision making. *MIS Quarterly*, *42*(2), 465–488. https://doi.org/10.25300/MISQ/2018/14316

Al-Natour, S., Cavusoglu, H., Benbasat, I., & Aleem, U. (2020). An empirical investigation of the antecedents and consequences of privacy uncertainty in the context of mobile apps. *Information Systems Research*, *31*(4), 1037–1063. https://doi.org/10.1287/isre.2020.0931

Avgerou, C. (2019). Contextual explanation: Alternative approaches and persistent challenges. *MIS Quarterly*, *43*(3), 977–1006. https://doi.org/10.25300/MISQ/2019/13990

Ayyagari, R., Grover, V., & Purvis, R. (2011). Technostress: Technological antecedents and implications. *MIS Quarterly*, *35*(4), 831–858. https://doi.org/10.2307/41409963

Bagozzi, R. P. (1980). *Causal models in marketing*. Wiley.

Bansal, G., Zahedi, F., & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems*, *49*(2), 138–150. https://doi.org/10.1016/j.dss.2010.01.010

Behrend, T. S., Sharek, D. J., Meade, A. W., & Wiebe, E. N. (2011). The viability of crowdsourcing for survey research. *Behavior Research Methods*, *43*(3), 800–813. https://doi.org/10.3758/s13428-011-0081-0

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly*, *35*(4), 1017–1042. https://doi.org/10.2307/41409971

Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: The role of privacy, security, and site attributes. *The Journal of Strategic Information Systems*, *11*(3–4), 245–270. https://doi.org/10.1016/S0963-8687(02)00018-5

Bélanger, F., & James, T. L. (2020). A theory of multilevel information privacy management for the digital era. *Information Systems Research*, *31*(2), 510–536. https://doi.org/10.1287/isre.2019.0900

Buhrmester, M., Kwang, T., & Gosling, S. D. (2011). Amazon's Mechanical Turk: A new source of inexpensive, yet high-quality, data? *Perspectives on Psychological Science*, *6*(1), 3–5. https://doi.org/10.1177/1745691610393980

Carter, M., Wright, R., Thatcher, J. B., & Klein, R. (2014). Understanding online customers' ties to merchants: The moderating influence of trust on the relationship between switching costs and e-loyalty. *European Journal of Information Systems*, *23*(2), 185–204. https://doi.org/10.1057/ejis.2012.55

Chellappa, R. K., & Sin, R. G. (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information Technology and Management*, *6*(2–3), 181–202. https://doi.org/10.1007/s10799-005-5879-y

Chen, R., & Sharma, S. K. (2013). Learning and self-disclosure behavior on social networking sites: The case of Facebook users. *European Journal of Information Systems*, *24*(1), 93–106. https://doi.org/10.1057/ejis.2013.31

Converse, J. M., & Presser, S. (1986). *Survey questions: Handcrafting the standardized questionnaire* (Vol. 63). Sage.

Crossler, R. E., & Bélanger, F. (2019). Why would i use location-protective settings on my smartphone? Motivating protective behaviors and the existence of the privacy knowledge–belief gap. *Information Systems Research*, *30*(3), 995–1006. https://doi.org/10.1287/isre.2019.0846

Crossler, R. E., & Posey, C. (2017). Robbing Peter to pay Paul: Surrendering privacy for security's sake in an identity ecosystem. *Journal of the Association for Information Systems*, *18*(7), 487–515. https://doi.org/10.17705/1jais.00463

Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues*, *59*(2), 323–342. https://doi.org/10.1111/1540-4560.00067

Cunningham, S. M. (1967). The major dimensions of perceived risk. In D. F. Cox (Ed.), *Risk taking and information handling in consumer behavior* (pp. 82–108). Harvard.

De Moya, J.-F., & Pallud, J. (2020). From panopticon to heautopticon: A new form of surveillance introduced by quantified-self practices. *Information Systems Journal*, *30*(6), 940–976. https://doi.org/10.1111/isj.12284

Degirmenci, K., Guhr, N., & Breitner, M. (2013, December 15–18). *Mobile applications and access to personal information: A discussion of users' privacy concerns*. In ICIS 2013 Proceedings, Milano, Italy. http://aisel.aisnet.org/icis2013/proceedings/SecurityOfIS/6

Delgado-Márquez, B. L., Hurtado-Torres, N. E., & Aragón-Correa, J. A. (2012). The dynamic nature of trust transfer: Measurement and the influence of reciprocity. *Decision Support Systems*, *54*(1), 226–234. https://doi.org/10.1016/j.dss.2012.05.008

DeVellis, R. F. (2003). *Scale development: Theory and applications*. Sage.

Diamantopoulos, A., & Siguaw, J. A. (2006). Formative versus reflective indicators in organizational measure development: A comparison and empirical illustration. *British Journal of Management*, *17*(4), 263–282. https://doi.org/10.1111/j.1467-8551.2006.00500.x

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., & Colautti, C. (2006). Privacy calculus model in e-commerce—A study of Italy and the United States. *European Journal of Information Systems*, *15*(4), 389–402. https://doi.org/10.1057/palgrave.ejis.3000590

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, *17*(1), 61–80. https://doi.org/10.1287/isre.l060.0080

Dinev, T., McConnell, A. R., & Smith, H. J. (2015). Research commentary—Informing privacy research through information systems, psychology, and behavioral economics: Thinking outside the "APCO" box. *Information Systems Research*, *26*(4), 639–655. https://doi.org/10.1287/isre.2015.0600

Dinev, T., Xu, H., Smith, H. J., & Hart, P. (2013). Information privacy and correlates: An empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems*, *22*(3), 295–316. https://doi.org/10.1057/ejis.2012.23

Dowling, G. R. (1986). Perceived risk: The concept and its measurement. *Psychology & Marketing*, *3*(3), 193–210. https://doi.org/10.1002/mar.4220030307

Edwards, J. R. (2001). Multidimensional constructs in organizational behavior research: An integrative analytical framework. *Organizational Research Methods*, *4*(2), 144–192. https://doi.org/10.1177/109442810142004

European Commission. (2016). *Flash Eurobarometer*. https://data.europa.eu/euodp/data/dataset/S2124_443_ENG

Faja, S., & Trimi, S. (2006). Influence of the web vendor's interventions on privacy-related behaviors in e-commerce. *Communications of the Association for Information Systems*, *17*, 2–68. https://doi.org/10.17705/1CAIS.01727

Featherman, M. S., & Pavlou, P. A. (2003). Predicting e-services adoption: A perceived risk facets perspective. *International Journal of Human-Computer Studies*, *59*(4), 451–474. https://doi.org/10.1016/S1071-5819(03)00111-3

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, *18*(1), 39–50. https://doi.org/10.2307/3151312

Gerlach, J., Buxmann, P., & Diney, T. (2019). "They're all the same!" stereotypical thinking and systematic errors in users' privacy-related judgments about online services. *Journal of the Association for Information Systems*, *20*(6), 787–823. https://doi.org/10.17705/1jais.00551

Ghosh, D. (2017). *AI is the future of hiring, but it's far from immune to bias*. Quartz. https://qz.com/work/1098954/ai-is-the-future-of-hiring-but-it-could-introduce-bias-if-were-not-careful/

Giaglis, G. M., Klein, S., & O'Keefe, R. M. (2002). The role of intermediaries in electronic marketplaces: Developing a contingency model. *Information Systems Journal*, *12*(3), 231–246. https://doi.org/10.1046/j.1365-2575.2002.00123.x

Glover, S., & Benbasat, I. (2010). A comprehensive model of perceived risk of e-commerce transactions. *International Journal of Electronic Commerce*, *15*(2), 47–78. https://doi.org/10.2753/JEC1086-4415150202

Goodman, J. K., & Paolacci, G. (2017). Crowdsourcing consumer research. *Journal of Consumer Research*, *44*(1), 196–210. https://doi.org/10.1093/jcr/ucx047

Gregor, S. (2006). The nature of theory in information systems. *MIS Quarterly*, *30*(3), 611–642. https://doi.org/10.2307/25148742

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2014). *Multivariate data analysis* (7th ed.). Pearson.

Hair, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2016). *A primer on partial least squares structural equation modeling (PLS-SEM)*. Sage.

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., Sarstedt, M., & Gudergan, S. P. (2018). *Advanced issues in partial least square structural equation modeling*. Sage.

Haug, M., Rössler, P., & Gewald, H. (2020, June 15–17). *How users perceive privacy and security risks concerning smart speakers*. In ECIS 2020 Research Papers, Marrakech, Morocco. https://aisel.aisnet.org/ecis2020_rp/129

Hille, P., Walsh, G., & Cleveland, M. (2015). Consumer fear of online identity theft: Scale development and validation. *Journal of Interactive Marketing*, *30*, 1–19. https://doi.org/10.1016/j.intmar.2014.10.001

Hinkin, T. R., & Tracey, J. B. (1999). An analysis of variance approach to content validation. *Organizational Research Methods*, *2*(2), 175–186. https://doi.org/10.1177/109442819922004

Hoehle, H., Aljafari, R., & Venkatesh, V. (2016). Leveraging Microsoft's mobile usability guidelines: Conceptualizing and developing scales for mobile application usability. *International Journal of Human-Computer Studies*, *89*(5), 35–53. https://doi.org/10.1016/j.ijhcs.2016.02.001

Hoehle, H., & Venkatesh, V. (2015). Mobile application usability: Conceptualization and instrument development. *MIS Quarterly*, *39*(2), 435–472. https://doi.org/10.25300/MISQ/2015/39.2.08

Hong, W., Chan, F. K. Y., Thong, J. Y. L., Chasalow, L. C., & Dhillon, G. (2013). A framework and guidelines for context-specific theorizing in information systems research. *Information Systems Research*, *25*(1), 111–136. https://doi.org/10.1287/isre.2013.0501

Hong, W., & Thong, J. Y. L. (2013). Internet privacy concerns: An integrated conceptualization and four empirical studies. *MIS Quarterly*, *37*(1), 275–298. https://doi.org/10.25300/MISQ/2013/37.1.12

Howell, D. C. (2013). *Statistical methods for psychology*. Cengage.

Hu, X., Wu, G., Wu, Y., & Zhang, H. (2010). The effects of web assurance seals on consumers' initial trust in an online vendor: A functional perspective. *Decision Support Systems*, *48*(2), 407–418. https://doi.org/10.1016/j.dss.2009.10.004

Hui, K.-L., Teo, H. H., & Lee, S.-Y. T. (2007). The value of privacy assurance: An exploratory field experiment. *MIS Quarterly*, *31*(1), 19–33. https://doi.org/10.2307/25148779

Hulland, J., & Miller, J. (2018). "Keep on turkin'"? *Journal of the Academy of Marketing Science*, *46*(5), 789–794. https://doi.org/10.1007/s11747-018-0587-4

Jacoby, J., & Kaplan, L. B. (1972, November 2-5). The components of perceived risk. *In Proceedings of the Third Annual Conference of the Association for Consumer Research*, Chicago, pp. 382–393. https://www.acrwebsite.org/assets/PDFs/Proceedings/NAACR3rdannual.pdf

Jarvis, C. B., MacKenzie, S. B., & Podsakoff, P. M. (2003). A critical review of construct indicators and measurement model misspecification in marketing and consumer research. *Journal of Consumer Research*, *30*(2), 199–218. https://doi.org/10.1086/376806

Jia, R., Steelman, Z. R., & Reich, B. H. (2017). Using Mechanical Turk data in IS research: Risks, rewards, and recommendations. *Communications of the Association for Information Systems*, *41*(1), 301–318. https://doi.org/10.17705/1CAIS.04114

Jiang, P., Jones, D. B., & Javie, S. (2008). How third-party certification programs relate to consumer trust in online transactions: An exploratory study. *Psychology and Marketing*, *25*(9), 839–858. https://doi.org/10.1002/mar.20243

Junglas, I. A., Johnson, N. A., & Spitzmüller, C. (2008). Personality traits and concern for privacy: An empirical study in the context of location-based services. *European Journal of Information Systems*, *17*(4), 387–402. https://doi.org/10.1057/ejis.2008.29

Karimi, J., & Walter, Z. (2015). The role of dynamic capabilities in responding to digital disruption: A factor-based study of the newspaper industry. *Journal of Management Information Systems*, *32*(1), 39–81. https://doi.org/10.1080/07421222.2015.1029380

Karwatzki, S., Dytynko, O., Trenz, M., & Veit, D. (2017). Beyond the personalization–privacy paradox: Privacy valuation, transparency features, and service personalization. *Journal of Management Information Systems*, *34*(2), 369–400. https://doi.org/10.1080/07421222.2017.1334467

Karwatzki, S., Trenz, M., Tuunainen, V. K., & Veit, D. (2017). Adverse consequences of access to individuals' information: An analysis of perceptions and the scope of organisational influence. *European Journal of Information Systems*, *26*(6), 688–715. https://doi.org/10.1057/s41303-017-0064-z

Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal*, *25*(6), 607–635. https://doi.org/10.1111/isj.12062

Keith, M. J., Babb, J. S., Lowry, P. B., Furner, C. P., & Abdullat, A. (2015). The role of mobile-computing self-efficacy in consumer information disclosure. *Information Systems Journal*, *25*(6), 637–667. https://doi.org/10.1111/isj.12082

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision Support Systems*, *44*(2), 544–564. https://doi.org/10.1016/j.dss.2007.07.001

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122–134. https://doi.org/10.1016/j.cose.2015.07.002

Kordzadeh, N., & Warren, J. (2017). Communicating personal health information in virtual health communities: An integration of privacy calculus model and affective commitment. *Journal of the Association for Information Systems*, *18*(1), 45–81. https://doi.org/10.17705/1jais.00446

KPMG. (2016, November 11). *Companies that fail to see privacy as a business priority risk crossing the 'creepy line.'*https://home.kpmg.com/sg/en/home/media/press-releases/2016/11/companies-that-fail-to-see-privacy-as-a-business-priority-risk-crossing-the-creepy-line.html

Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: Why we disclose. *Journal of Information Technology*, *25*(2), 109–125. https://doi.org/10.1057/jit.2010.6

Krosnick, J. A. (1991). Response strategies for coping with the cognitive demands of attitude measures in surveys. *Applied Cognitive Psychology*, *5*(3), 213–236. https://doi.org/10.1002/acp.2350050305

Lanzing, M. (2019). "Strongly recommended" revisiting decisional privacy to judge hypernudging in self-tracking technologies. *Philosophy & Technology*, *32*(3), 549–568. https://doi.org/10.1007/s13347-018-0316-4

Law, K. S., Wong, C.-S., & Mobley, W. M. (1998). Toward a taxonomy of multidimensional constructs. *Academy of Management Review*, *23*(4), 741–755. https://doi.org/10.5465/amr.1998.1255636

Lee, A., & Baskerville, R. L. (2012). Conceptualizing generalizability: New contribution and a reply. *MIS Quarterly*, *36*(3), 749–761. https://doi.org/10.2307/41703479

Leidner, D., & Tona, O. (2021). The CARE theory of dignity amid personal data digitalization. *MIS Quarterly*, *45*(1), 343–370. https://doi.org/10.25300/MISQ/2021/15941

Li, H., Sarathy, R., & Xu, H. (2010). Understanding situational online information disclosure as a privacy calculus. *Journal of Computer Information Systems*, *51*(1), 62–71. https://doi.org/10.1080/08874417.2010.11645450

Li, T., & Unger, T. (2012). Willing to pay for quality personalization? Trade-off between quality and privacy. *European Journal of Information Systems*, *21*(6), 621–642. https://doi.org/10.1057/ejis.2012.13

Li, Y. (2014). The impact of disposition to privacy, website reputation and website familiarity on information privacy concerns. *Decision Support Systems*, *57*, 343–354. https://doi.org/10.1016/j.dss.2013.09.018

Libaque-Sáenz, C. F., Wong, S. F., Chang, Y., & Bravo, E. R. (2021). The effect of fair information practices and data collection methods on privacy-related behaviors: A study of mobile apps. *Information & Management*, *58*(1), 103284. https://doi.org/10.1016/j.im.2020.103284

Little, T. D., Lindenberger, U., & Nesselroade, J. R. (1999). On selecting indicators for multivariate measurement and modeling with latent variables: When "good" indicators are bad and "bad" indicators are good. *Psychological Methods*, *4*(2), 192–211. https://doi.org/10.1037/1082-989X.4.2.192

Liu, Z., Wang, X., Min, Q., & Li, W. (2019). The effect of role conflict on self-disclosure in social network sites: An integrated perspective of boundary regulation and dual process model. *Information Systems Journal*, *29*(2), 279–316. https://doi.org/10.1111/isj.12195

Lowry, P. B., Cao, J., & Everard, A. (2011). Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: The case of instant messaging in two cultures. *Journal of Management Information Systems*, *27*(4), 163–200. https://doi.org/10.2753/MIS0742-1222270406

Lowry, P. B., D'Arcy, J., Hammer, B., & Moody, G. D. (2016). "Cargo Cult" science in traditional organization and information systems survey research: A case for using nontraditional methods of data collection, including Mechanical Turk and online panels. *The Journal of Strategic Information Systems*, *25*(3), 232–240. https://doi.org/10.1016/j.jsis.2016.06.002

Lowry, P. B., Vance, A., Moody, G. D., Beckman, B., & Read, A. S. (2008). Explaining and predicting the impact of branding alliances and web site quality on initial consumer trust of e-commerce web sites. *Journal of Management Information Systems*, *24*(4), 199–224. https://doi.org/10.2753/MIS0742-1222240408

Luo, X., Li, H., Zhang, J., & Shim, J. P. (2010). Examining multi-dimensional trust and multi-faceted risk in initial acceptance of emerging technologies: An empirical study of mobile banking services. *Decision Support Systems*, *49*(2), 222–234. https://doi.org/10.1016/j.dss.2010.02.008

MacKenzie, S. B., Podsakoff, P. M., & Podsakoff, N. P. (2011). Construct measurement and validation procedures in mis and behavioral research: Integrating new and existing techniques. *MIS Quarterly*, *35*(2), 293–334. https://doi.org/10.2307/23044045

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, *15*(4), 336–355. https://doi.org/10.1287/isre.1040.0032

Miltgen, C. L., & Smith, H. J. (2015). Exploring information privacy regulation, risks, trust, and behavior. *Information & Management*, *52*(6), 741–759. https://doi.org/10.1016/j.im.2015.06.006

Mitchell, V.-W. (1999). Consumer perceived risk: Conceptualisations and models. *European Journal of Marketing*, *33*(1/2), 163–195. https://doi.org/10.1108/03090569910249229

Moise, I. (2018, March 28). What's on your mind? Bosses are using artificial intelligence to find out. *Wall Street Journal*. https://www.wsj.com/articles/whats-on-your-mind-bosses-are-using-artificial-intelligence-to-find-out-1522251302

Moore, G. C., & Benbasat, I. (1991). Development of an instrument to measure the perceptions of adopting an information technology innovation. *Information Systems Research*, *2*(3), 192–222. https://doi.org/10.1287/isre.2.3.192

Nickerson, R. C., Varshney, U., & Muntermann, J. (2013). A method for taxonomy development and its application in information systems. *European Journal of Information Systems*, *22*, 336–359. https://doi.org/10.1057/ejis.2012.26

Nunnally, J. C., & Bernstein, I. H. (1994). *Psychometric theory* (3rd ed.). McGraw-Hill.

Ogbanufe, O., & Gerhart, N. (2020). The mediating influence of smartwatch identity on deep use and innovative individual performance. *Information Systems Journal*, *30*(6), 977–1009. https://doi.org/10.1111/isj.12288

Oppenheimer, D. M., Meyvis, T., & Davidenko, N. (2009). Instructional manipulation checks: Detecting satisficing to increase statistical power. *Journal of Experimental Social Psychology*, *45*, 867–872. https://doi.org/10.1016/j.jesp.2009.03.009

Ozdemir, Z. D., Jeff Smith, H., & Benamati, J. H. (2017). Antecedents and outcomes of information privacy concerns in a peer context: An exploratory study. *European Journal of Information Systems*, *26*(6), 642–660. https://doi.org/10.1057/s41303-017-0056-z

Park, S., & Tussyadiah, I. P. (2017). Multidimensional facets of perceived risk in mobile travel booking. *Journal of Travel Research*, *56*(7), 854–867. https://doi.org/10.1177/0047287516675062

Peer, E., Vosgerau, J., & Acquisti, A. (2014). Reputation as a sufficient condition for data quality on Amazon Mechanical Turk. *Behavior Research Methods*, *46*(4), 1023–1031. https://doi.org/10.3758/s13428-013-0434-y

Polites, G. L., Roberts, N., & Thatcher, J. (2012). Conceptualizing models using multidimensional constructs: A review and guidelines for their use. *European Journal of Information Systems*, *21*(1), 22–48. https://doi.org/10.1057/ejis.2011.10

Raghavan, M., Barocas, S., Kleinberg, J., & Levy, K. (2020, January 27–30). *Mitigating bias in algorithmic hiring: Evaluating claims and practices*. In Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency, Barcelona, Spain, pp. 469–481. https://doi.org/10.1145/3351095.3372828

Savage, N. (2020). The race to the top among the world's leaders in artificial intelligence. *Nature*, *588*(7837), S102–S104. https://doi.org/10.1038/d41586-020-03409-8

Schmoll, R., & Bader, V. (2019, December 15–18). *Who or what screens which one of me? The differential effects of algorithmic social media screening on applicants' job pursuit intention*. In ICIS 2019 Proceedings, Munich, Germany. https://aisel.aisnet.org/icis2019/future_of_work/future_work/10

Sheehan, K., & Pittman, M. (2016). *Amazon's Mechanical Turk for academics: The HIT handbook for social science research*. Melvin & Leigh, Publishers.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, *35*(4), 989–1016. https://doi.org/10.2307/41409970

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly*, *20*(2), 167–196. https://doi.org/10.2307/249477

Spiekermann, S., Böhme, R., Acquisti, A., & Hui, K.-L. (2015). Personal data markets. *Electronic Markets*, *25*(2), 91–93. https://doi.org/10.1007/s12525-015-0190-1

Steelman, Z. R., Hammer, B. I., & Limayem, M. (2014). Data collection in the digital age: Innovative alternatives to student samples. *Journal of Consumer Psychology*, *23*(2), 212–219. https://doi.org/10.25300/MISQ/2014/38.2.02

Stone, R. N., & Grønhaug, K. (1993). Perceived risk: Further considerations for the marketing discipline. *European Journal of Marketing*, *27*(3), 39–50. https://doi.org/10.1108/03090569310026637

Straub, D., Boudreau, M.-C., & Gefen, D. (2004). Validation guidelines for is positivist research. *Communications of the Association for Information Systems*, *2004*(13), 380–427. https://doi.org/10.17705/1CAIS.01324

Sutanto, J., Palme, E., Tan, C.-H., & Phang, C. W. (2013). Addressing the personalization-privacy paradox: An empirical assessment from a field experiment on smartphone users. *MIS Quarterly*, *37*(4), 1141–1164. https://doi.org/10.25300/MISQ/2013/37.4.07

Teubner, T., & Flath, C. M. (2019). Privacy in the sharing economy. *Journal of the Association for Information Systems*, *20*(3), 213–242. https://doi.org/10.17705/1jais.00534

Trang, S., Trenz, M., Weiger, W. W., Tarafdar, M., & Cheung, C. M. K. (2020). One app to trace them all? Examining app specifications for mass acceptance of contact-tracing apps. *European Journal of Information Systems*, *29*(4), 415–428. https://doi.org/10.1080/0960085X.2020.1784046

Treiblmaier, H., & Pollach, I. (2007, December 9–12). *Users' perceptions of benefits and costs of personalization*. In ICIS 2007 Proceedings, Montreal, Canada. https://aisel.aisnet.org/icis2007/141/

TRUSTe. (2016). *2015 US consumer confidence infographic*. TRUSTe. https://www.truste.com/resources/privacy-research/us-consumer-confidence-index-2015/

van Slyke, C., Shim, J. T., Johnson, R., & Jiang, J. (2006). Concern for information privacy and online consumer purchasing. *Journal of the Association for Information Systems*, *7*(6), 415–444. https://doi.org/10.17705/1jais.00092

Verhagen, T., Meents, S., & Tan, Y.-H. (2006). Perceived risk and trust associated with purchasing at electronic marketplaces. *European Journal of Information Systems*, *15*(6), 542–555. https://doi.org/10.1057/palgrave.ejis.3000644

Walsh, G., Hille, P., Shiu, E., Hassan, L., & Takahashi, I. (2018, June 30–July 3). *Cross-cultural fear of online identity theft: A comparison study and scale refinement*. In ICIS 2018 Proceedings, Philadelphia, USA. https://aisel.aisnet.org/icis2018/security/Presentations/1

Walsh, I., Gettler-Summa, M., & Kalika, M. (2016). Expectable use: An important facet of IT usage. *The Journal of Strategic Information Systems*, *25*(3), 177–210. https://doi.org/10.1016/j.jsis.2016.01.003

Weber, R. (2003). Editor's comments: Still desperately seeking the IT artifact. *MIS Quarterly*, *27*(2), iii–xi.

Wright, R. T., Campbell, D. E., Thatcher, J. B., & Roberts, N. H. (2012). Operationalizing multidimensional constructs in structural equation modeling: Recommendations for IS research. *Communications of the Association for Information Systems*, *30*, 367–412. https://doi.org/10.17705/1CAIS.03023

Wu, Y., Ryan, S., & Windsor, J. (2009, December 15–18). *Influence of social context and affect on individuals' implementation of information security safeguards*. ICIS 2009 Proceedings, Phoenix, USA. http://aisel.aisnet.org/icis2009/70

Xu, C., Peak, D., & Prybutok, V. (2015). A customer value, satisfaction, and loyalty perspective of mobile application recommendations. *Decision Support Systems*, *79*, 171–183. https://doi.org/10.1016/j.dss.2015.08.008

Xu, H., Dinev, T., Smith, H., & Hart, P. (2008, December 14–17). *Examining the formation of individual's privacy concerns: Toward an integrative view*. In ICIS 2008 Proceedings, Paris, France. http://aisel.aisnet.org/icis2008/6

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems*, *12*(12), 798–824. https://doi.org/10.17705/1jais.00281

Xu, H., Teo, H.-H., Tan, B. C. Y., & Agarwal, R. (2009). The role of push–pull technology in privacy calculus: The case of location-based services. *Journal of Management Information Systems*, *26*(3), 135–173. https://doi.org/10.2753/MIS0742-1222260305

Yaraghi, N., Gopal, R. D., & Ramesh, R. (2019). Doctors' orders or patients' preferences? Examining the role of physicians in patients' privacy decisions on health information exchange platforms. *Journal of the Association for Information Systems*, *20*(7), 928–952. https://doi.org/10.17705/1jais.00557

Yun, H., Lee, G., & Kim, D. J. (2019). A chronological review of empirical research on personal information privacy concerns: An analysis of contexts and research constructs. *Information & Management*, *56*(4), 570–601. https://doi.org/10.1016/j.im.2018.10

Zhang, N., Wang, C. (. A.)., Karahanna, E., & Xu, Y. (2022). Peer privacy concerns: Conceptualization and measurement. *MIS Quarterly*, *46*(1), 491–530. https://doi.org/10.25300/MISQ/2022/14861

AUTHOR BIOGRAPHIES

Sabrina Karwatzki is a research fellow at the Chair of Information Systems and Management at the Faculty of Business and Economics of University of Augsburg, Germany. She received her Ph.D. from the Business School of the University of Mannheim, Germany. She is interested in the role information privacy plays in today's society. Therefore, her research focusses on the impact of information privacy on individuals' behaviour and organisations' practices. Her work appears in journals including the *European Journal of Information Systems*, *Journal of Management Information Systems and Journal of Business Economics* and in conference proceedings such as ECIS and HICSS. Sabrina is currently working as a specialist in data & analytics governance at Schaeffler AG.

Manuel Trenz is Professor for Interorganizational Information Systems at the University of Goettingen, Germany. He holds a Ph.D. from the Business School of the University of Mannheim, Germany. His research is dedicated to the study and advancement of data-driven innovation and digital platforms. He is particularly interested in how people interact in data-intensive contexts and how data can be used in prudent ways for innovation and algorithmic decision making. His work has appeared in journal such as *MIS Quarterly*, *Journal of Management Information Systems*, *European Journal of Information Systems*, *Internet Research*, *Information & Management*, *Business & Information Systems Engineering*, and others. He co-edited the ISJ special issue on 'The Digitization of the

Individual', which appeared in 2020, and serves as an Associate Editor on the editorial board of the *Information Systems Journal*.

Daniel Veit is currently a full professor and Chair of Information Systems and Management at the Department of Business Administration of the Faculty of Business and Economics of the University of Augsburg, Germany. His research focusses on transformational effects of information systems and digitalisation in society with a specific focus on sustainability. His publications have appeared in outlets such as the *MIS Quarterly*, *Journal of Management Information Systems*, *European Journal of Information Systems*, *Journal of Service Research*, *Information & Management*, *Internet Research*, *MIS Quarterly Executive*, *Journal of Business Economics* and *Business & Information Systems Engineering*. He co-edited the *ISJ* Special Issue on 'Digitization in Business Models and Entrepreneurship', which appeared in 2016. He serves as a Senior Editor on the editorial board of the *Journal of the Association for Information Systems* as well as an Associate Editor on the editorial board of the *Information Systems Journal*. During the past 15 years he served, amongst others, as Associate Dean for international affairs and Academic Director of the ESSEC & Mannheim Executive MBA program at Mannheim Business School, Germany and held a number of guest professor positions at international business schools.

SUPPORTING INFORMATION

Additional supporting information may be found in the online version of the article at the publisher's website.

How to cite this article: Karwatzki, S., Trenz, M., & Veit, D. (2022). The multidimensional nature of privacy risks: Conceptualisation, measurement and implications for digital services. *Information Systems Journal*, *32*(6), 1126–1157. https://doi.org/10.1111/isj.12386