Public Information Sharing in Enterprise Social Networks: A Communication Privacy Management Perspective

Yu Wang[a], *Daqing Zheng*[a]*, *Yulin Fang*[b]

[a] School of Information Management and Engineering, Shanghai University of Finance and Economics, Shanghai, China

[b] Business School, The University of Hong Kong, Hong Kong, China

* Corresponding author.

E-mail addresses: wangyu_12edu@163.com (Y. Wang), zhengdaqing@sina.com (D. Zheng), ylfang@hku.hk (Y.Fang)

Public Information Sharing in Enterprise Social Networks: A Communication Privacy Management Perspective

Abstract

Purpose – The advancement of enterprise social networks (ESNs) facilitates information sharing, yet also presents the challenge of managing information boundaries. This study aims to explore the factors that influence the information control behavior of ESN users when continuously sharing information.

Design/methodology/approach – This study specifies the information control behaviors in the "wall posts" channel and applies communication privacy management (CPM) theory to analyze the effects of the individual-specific factor (disposition to value information), context-specific factors (work-relatedness and information richness), and risk-benefit ratio (public benefit and public risk). Data on actual information control behaviors extracted from ESN logs are examined using multilevel mixed-effects logistic regression analysis.

Findings – Study findings show the direct effects of the individual-specific factor, context-specific factors, and risk-benefit ratio, highlighting interactions between the individual motivation factor and ESN context factors.

Originality/value – This study reshapes the relationship of CPM theory boundary rules in the ESN context, extending information-control research and providing insights into ESNs' information-control practices.

Keywords Enterprise social networks, Information sharing, Information control, Communication privacy management theory, Multilevel mixed-effects logistic regression

Paper type Research paper

1. Introduction

The adoption of social networks (SNs) like Meta (Facebook), WeChat, and Twitter in the business environment has spawned enterprise social networks (ESNs). Enterprise-led information technology (IT) platforms such as Workplace, WeCom, and DingTalk allow employees to share information and collaborate (Leonardi, 2015; Wang *et al.*, 2019). The COVID-19 pandemic has further increased the

adoption of ESNs, wherein 81% of enterprises and nearly 100% of Fortune 500 companies use ESNs to share information (Goswami, 2023). ESNs effectively enable information sharing, but their rapid information dissemination poses challenges for information boundary management (Zhou *et al.*, 2023). ESN users need to be mindful of information boundary management, as incorrectly managed information boundaries can cause serious problems. For example, in 2021, a misconfiguration in Microsoft Power Apps' setting led to 38 million pieces of sensitive information being exposed, affecting American Airlines, J.B. Hunt, and several government bodies. Microsoft then changed the default "keep publicly accessible" information control setting on Power Apps (Endicott, 2021).

Information sharing in ESNs, which involves two or more employees cooperating to exchange information (Laitinen and Sivunen, 2020), puts enterprises at risk of confidential information leakage (Golbeck, 2015), thereby justifying the study of information control in ESN contexts. Reducing information risk does not mean hiding information completely, but rather effectively managing information boundaries and controlling information access (Lin and Armstrong, 2019). Information control is the right to create information boundaries that limit access to personal information (Golbeck, 2015). Most ESNs feature information control settings that can help users avoid confidential information leakage (Schwartz-Chassidim *et al.*, 2020).

While researchers have increasingly recognized the importance of information control in ESNs (Fiesler *et al.*, 2017), the emerging contexts and hard-to-observe information-control practices in ESNs pose three key challenges for studying information control behaviors. First, most studies have explored the disclosure of ESN users' identity, workplace, and location (Chen *et al.*, 2020; Li *et al.*, 2020; Pu *et al.*, 2020), which parallels Internet privacy in general SNs (Ball *et al.*, 2012), and are highly correlated with personal attributes. They failed, however, to capture the business attributes of information privacy in ESN information control, which if not managed properly, can lead to confidential information leakage (Bélanger and James, 2020; Golbeck, 2015). Second, existing studies have focused on a crucial information-sharing channel, "profile pages" (Venkatanathan *et al.*, 2014), while considering information control in ESNs as static information disclosure on these profile pages. What they ignored is the non-stop information broadcasting that occurs in channels such as "wall posts" (Venkatanathan *et al.*, 2014), where ESN users

continuously employ different information control settings that evolve to adapt to specific contexts (Wang *et al.*, 2022). Finally, some studies have focused on users' sentiments (e.g., psychological expressions) when voicing concerns about information leakage, where they have reported intentions that were unverified (Habib *et al.*, 2019; Wang and Fussell, 2020). Users' actual behaviors, however, rarely reflect this level of anxiety (Keith *et al.*, 2014), a discrepancy known as the "privacy paradox" (Barth and de Jong, 2017; Duan and Deng, 2022). This underscores the need to use actual behaviors to accurately identify the mechanisms underlying users' information control in ESNs.

With increased attention to information control, some theories employed include privacy calculus proposed by Laufer and Wolfe (1977). They argued that willingness to share information is based on a rational trade-off between perceived risks and expected benefits, where individuals will share information when they perceive such benefits are worth the risks (Chen, 2018; Dinev and Hart, 2006). Privacy calculus, however, does not explain how risks and benefits work together in any given context, making it difficult to identify more factors that can explain the information privacy phenomenon, especially in the current IT environment. Anderson and Agarwal (2011) and Chen *et al.* (2020) suggested that the communication privacy management (CPM) theory, which incorporates other factors that emphasize motivation and context, is needed to gain a comprehensive understanding of information privacy issues. CPM theory is a framework developed by Petronio (1991) to fully explain how individuals manage their information boundaries and decide with whom to share information. The theory's emphasis on how boundary control should be responsive to immediate changes in context is highly relevant to ESN user practices, which emphasize the need to adapt information control strategies to specific contexts. The theory describes the core maxim of information boundaries and clarifies criteria such as motivation (the intrinsic impetus to maintain boundaries), context and its immediate changes, and the risk-benefit ratio when governing such boundaries (Petronio and Durham, 2015).

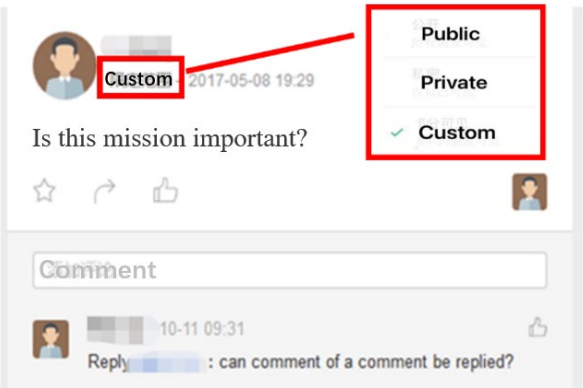

Figure 1. Information control settings in wall posts

Source(s): Author's own creation/work

This study focuses on wall posts that provide users with an information control interface to choose between public, private, and custom settings (Figure 1). Given the work-oriented nature of ESNs and the business communication function of the wall posts channel, the study merges private settings (which are rarely found in practice) into custom settings and explores this public-custom binary (Fiesler *et al.*, 2017; Golbeck, 2015). The study first applies CPM theory to theorize the factors affecting users' public sharing behavior and develops a model incorporating interaction effects. The model shows that users' disposition to value information refers to how users dispose of different information (Bassellier *et al.*, 2015), reflecting their intrinsic need to manage information boundaries (Xu *et al.*, 2011). Work-relatedness and information richness (which reflect immediate changes in the ESN context) can improve users' understanding of information control issues (Xu *et al.*, 2011). Such understanding may override their pre-existing disposition to value information (Kehr *et al.*, 2013. The risk-benefit ratio is also crucial (Chen *et al.*, 2020; Li *et al.*, 2020; Lin and Armstrong, 2019). The study validates the information control strategy using actual behavioral data, and the results mainly confirm the direct and interaction effects. The study deepens the theoretical research on CPM theory, expands the research boundaries of information control behavior, and can guide user information-control practices.

2. Theoretical background

ESNs users' information control behavior is related to information control in ESNs and CPM theory. This study explores the research and findings in these two areas.

2.1 Information control in ESNs

Information control in SNs asserts the individuals' right to control information, allowing them to create information boundaries that limit others' access and reduce information leakage risk (Golbeck, 2015). SN users rely on information control settings to target specific audiences (Schwartz-Chassidim *et al.*, 2020), settings that are also used in ESNs. ESNs are the socialization of the enterprise, and integrate SNs into the workplace (Wang *et al.*, 2019). Their work-oriented nature prevents the autonomy that general SNs afford, as employees must authenticate using real names and preclude information sharing across multiple accounts (Vitak *et al.*, 2012). ESN users are thus more concerned about confidential information leakage (Golbeck, 2015; Smith and Brunner, 2017). SN users can avoid information leakage by not sharing, but due to business processes, employees must share certain confidential information, making proper information control settings even more important (Lin and Armstrong, 2019). Furthermore, ESNs' information control focuses more on task- and project-related business attributes of information privacy in work scenarios than on highly private attributes of Internet privacy (e.g., real name and address) in SNs (Ball *et al.*, 2012). These distinctions reinforce the need to study information control in the ESN-specific context (Vitak *et al.*, 2012).

Research on information control in ESNs has revealed three main trends. First, studies have mainly focused on Internet privacy rather than information privacy in work scenarios (Ball *et al.*, 2012). They discussed the fixed information disclosures posted on profile pages and the privacy risks arising from sharing information such as identity, workplace, and location (Chen *et al.*, 2020; Li *et al.*, 2020; Pu *et al.*, 2020; Wang *et al.*, 2022). They did not address continuous information sharing or the adaptability of information control to changes in information privacy under specific contexts (Bélanger and James, 2020). Second, the antecedents of information control have not received sufficient attention, as most studies explored the endogenous and exogenous reasons for users' information sharing (Laitinen and Sivunen, 2020; Smith and Brunner, 2017). Choosing an appropriate information control setting, however, has been viewed as superior for protecting information than not sharing it at all (Lin and Armstrong, 2019). That is, merely looking at whether users share information does not fully explain the information-sharing phenomenon (Schwartz-Chassidim *et al.*, 2020). Third, a few studies on information control focused on users' reported

sentiments and intentions without subjective verification (Keith *et al.*, 2014; Wang and Fussell, 2020). Wang and Fussell (2020) conducted interviews to ascertain participants' privacy attitudes and noted that information control is a cognitive process that depends on information perception. The privacy paradox has indicated considerable differences between expressed attitudes and actual behaviors (Barth and de Jong, 2017), thus confirming how information control intentions are poor predictors of behavior (Acquisti and Grossklags, 2004; Keith *et al.*, 2014). This highlights the importance of using actual information control behaviors rather than self-reported surveys (Schwartz-Chassidim *et al.*, 2020). Furthermore, ESNs users need to put more effort into their use of information control settings, yet little research has focused on this complex mechanism.

This study focuses on a specific aspect of information control behaviors in ESNs: how employees manage shared information in their wall posts using information control settings, which manifest as whether to share information publicly in immediately changing contexts. This study points out the importance of using actual behavioral data to analyze users' information control mechanisms in ESNs. Exploring the public-custom binary is still a reasonable approach (Fiesler *et al.*, 2017; Golbeck, 2015), although such mechanisms are complex. This is because the work-oriented nature and drive for business communication in ESN wall posts lead employees to limit their use of the private option.

2.2 CPM theory

Petronio's (1991) CPM theory explains information-sharing decisions by incorporating complex concepts of information boundary, boundary coordination, and boundary turbulence while asserting that individuals can determine with whom to co-own information. The core maxim is the shared information boundary, which is co-created between owners and confidants who have control over access to information (Hinde and Ophoff, 2020). Shared information boundaries vary from being completely open to closed depending on the situation, thereby allowing for information to be shared publicly or kept private (Xu *et al.*, 2011). The boundary thickens when public sharing is undesirable and information flow is restricted, and thins when public sharing is encouraged and information flows freely (Petronio and Durham, 2015; Xu *et al.*, 2011).

CPM theory articulates five boundary rules, categorized as "core" and "catalytic" (Petronio and Durham, 2015). Core rules are more durable and include cultural values and gender orientation,

whereas the catalytic rules include motivation, context, and risk-benefit ratio, which are more responsive to changes as circumstances require. The current study focuses on catalytic rules, as cultural values are not considered due to cultural homogeneity (Li *et al.*, 2020; Xu *et al.*, 2011), and gender is included as a control variable (Lin and Armstrong, 2019; Liu and Wang, 2018; Xu *et al.*, 2011).

Motivation and context are found to influence information boundary formation (Petronio, 1991; Petronio, 2002). Motivation reflects the individual intrinsic need to maintain information boundaries (Karwatzki *et al.*, 2017; Xu *et al.*, 2011), which is linked to an individual-specific factor and is associated with dyadic effects, reciprocity, and rewards (Petronio, 2002). Factors such as trust (Petronio, 1991; Petronio, 2002), commitment, reputation (Chen *et al.*, 2020), and the disposition to value information (Kehr *et al.*, 2013; Liu and Wang, 2018; Xu *et al.*, 2011) have been identified as individual-specific. Context is shaped by physical, social, and environmental factors (Petronio, 1991), while shocks-to-life circumstances can explain changes in immediate demand in certain situations, such as a new work environment or a new business process (Petronio, 2002). This study explores an ESN wherein users' physical and social macro-environment converges. The research is aligned with Laitinen and Sivunen's (2020) finding: immediate changes in context will pertain to the users' perceived micro-environment during information sharing (Xu *et al.*, 2011). CPM theory also proposes that coexisting benefits and risks affect information boundaries (Petronio, 2002), where benefits can include self-presentation (Min and Kim, 2015), satisfying needs (Christofides *et al.*, 2009), or gaining recognition (Christofides *et al.*, 2009; Li *et al.*, 2020); risks are potential losses (Malhotra *et al.*, 2004; Xu *et al.*, 2011) such as information leakage or misuse (Chen *et al.*, 2020).

CPM theory has been applied to explain information privacy issues arising from new IT (Anderson and Agarwal, 2011; Li *et al.*, 2020; Lin and Armstrong, 2019). It is also applicable when exploring employees' perceptions of privacy violations (Hinde and Ophoff, 2020) or context-specific limitations of information disclosure in the workplace (Smith and Brunner, 2017). Researchers who have applied CPM theory to ESNs, however, have focused more on information-sharing intentions, including facilitators and limitations of information-sharing (Laitinen and Sivunen, 2020). They did not incorporate information control behaviors or consider that information control should be adapted to contextual changes. Furthermore, existing studies generally explored

the independent effects of each boundary rule (Chen *et al.*, 2020; Laitinen and Sivunen, 2020; Li *et al.*, 2020) and reveal little about possible internal associations (Anderson and Agarwal, 2011; Krämer and Haferkamp, 2011; Lin and Armstrong, 2019). There have been calls to explore how motivational factors are overridden by contextual conditions, however (Kehr *et al.*, 2013). These points have served as directions for the application and development of CPM theory in this study.

3. Research model and hypotheses

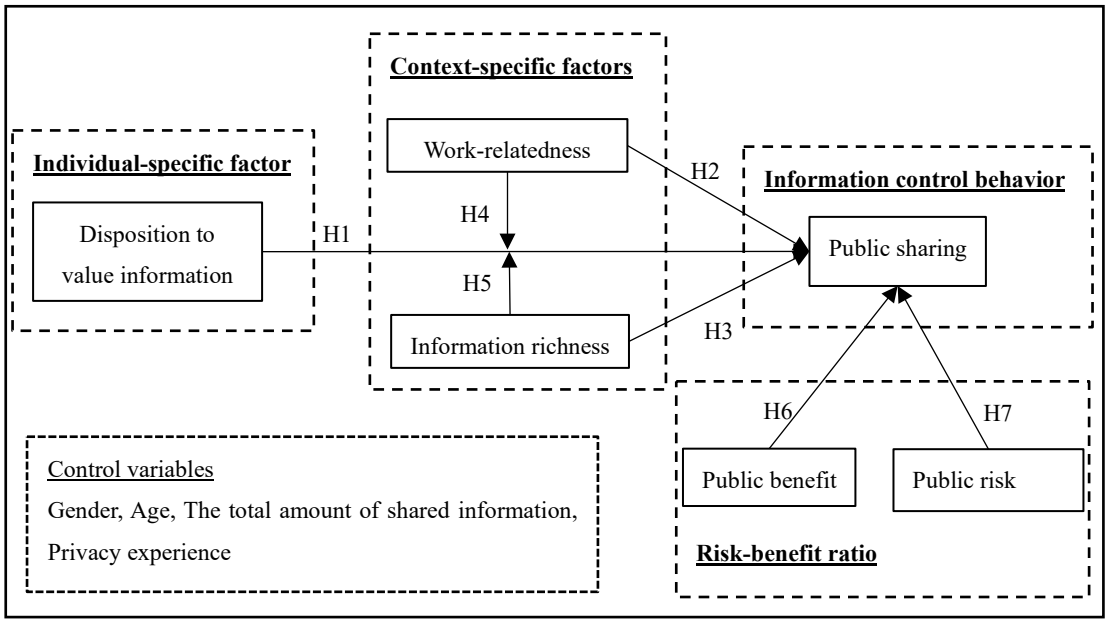

Figure 2. Research model

Source(s): Author's own creation/work

The proposed research model is based on ESN information control research and CPM theory, as shown in Figure 2. It focuses on the three boundary rules that determine public sharing: the individual-specific factor (disposition to value information), context-specific factors (work-relatedness and information richness), and risk-benefit ratio (public benefit and public risk). Previous studies have explored the disposition to value information (Bassellier *et al.*, 2015) and its relation to public sharing (Liu and Wang, 2018; Malhotra *et al.*, 2004). Information control issues are better understood in specific contexts (Xu *et al.*, 2011), and factors such as work-relatedness and information richness need to be considered. Following Anderson and Agarwal (2011), this study designates context-specific factors as moderators and expects them to interact with the disposition to value information in influencing public sharing. Lastly, individuals perform "mental calculus"

when managing information boundaries through trade-offs between benefits and risks (Laufer and Wolfe, 1977).

3.1 Disposition to value information and public sharing

This study applies disposition to value information to the general practices of ESN users to protect the "information space" (Xu *et al.*, 2011), which is initially concerned with awareness and perceptions related to information leakage (Campbell, 1997). Disposition to value information is the individual-specific factor that contributes to boundary formation (Petronio, 2002). Barth and de Jong (2017) proposed that information boundary decisions are driven by the disposition to value information (Kehr *et al.*, 2013; Xu *et al.*, 2011). Users inherently pay attention to information differently and show varied information disposal practices. The more attention users pay to information, the more cautious they are in information sharing, thus displaying a higher disposition to value information.

Information privacy studies have indeed confirmed that users with a high disposition to value information are deeply concerned about information privacy (Malhotra *et al.*, 2004) and are more likely to limit sharing to avoid social punishment or disapproval (Min and Kim, 2015). Such users also exhibit higher IT proficiency (Bassellier *et al.*, 2015), as those with greater knowledge of ESN functions will be more likely to use them to discreetly dispose of information (Saraf *et al.*, 2007; Schwartz-Chassidim *et al.*, 2020; Xu *et al.*, 2011). In contrast, those with a low disposition to value information are less concerned with controlling information, do not seek to understand ESN functions, and tend to share information more widely (Saraf *et al.*, 2007; Xu *et al.*, 2011). Moreover, Malhotra *et al.* (2004) demonstrated that users with higher concern for privacy were less likely to trust information sources (Chen, 2018), despite not finding a direct effect of the disposition to value information on information-sharing behavior. Regardless, it can be inferred that users with a higher disposition to value information in ESNs will limit boundaries when sharing information and are less likely to share it publicly (Saraf *et al.*, 2007). This study thus proposes the following hypothesis:

H1. Users' disposition to value information in ESNs is negatively related to public sharing. Specifically, the higher the disposition to value information, the less likely users are to share information publicly.

3.2 Work-relatedness, information richness, and public sharing

Information sharing on work-oriented ESNs is greatly impacted by the context of the content (Laitinen and Sivunen, 2020). Work-related information on such platforms is a context-specific factor, and studies have shown that some users will share more work-related information to complete work due to the visibility of ESNs (Forsgren and Byström, 2018; Yang *et al.*, 2021). Non-work-related information sharing can nonetheless positively affect employees' organizational engagement (Zhang *et al.*, 2019) and innovation performance (Sun *et al.*, 2021), leading users to appropriately share such information. Different information control settings are used for work-related and non-work-related information for effective communication and privacy protection (Sun *et al.*, 2021). The professional aspect of work-related information, however, suggests it is usually not shared publicly (Fox and McEwan, 2017; Liu and Kang, 2017) due to its sensitivity (Anderson and Agarwal, 2011; Malhotra *et al.*, 2004). Liu and Kang's (2017) online experiment found that ESNs stimulate employees to share professional information with specific colleagues. Such custom sharing of information leads to more interpersonal attribution and projects a professional image that can gain respect from colleagues (Lee *et al.*, 2019; Liu and Kang, 2017). Information privacy in work scenarios reflects important context considerations (Smith *et al.*, 2011), as work-related information is often more sensitive (Anderson and Agarwal, 2011). Malhotra *et al.* (2004) and Anderson and Agarwal (2011) argued that all else being equal, sensitive information is more threatening to user information security (Cichy *et al.*, 2021), negatively affecting users' public sharing in ESNs. This study therefore proposes:

H2. In the ESN context, work-related information is negatively related to users' public sharing. Specifically, for work-related information, users are less likely to share it publicly.

Another important factor of ESNs is information richness, as supported by the media richness theory (MRT) proposed by Daft and Lengel (1986). MRT emphasizes the ability of the media's information load to facilitate understanding, wherein information richness manifests as differences between required and available information (i.e., uncertainty), and multiple conflicting interpretations (i.e., equivocality). ESNs can avoid such conflicting values (Krämer and Haferkamp, 2011) by properly managing information uncertainty (Yee *et al.*, 2021) and providing equivocal information. High information richness leads to low uncertainty and is more likely to be misused

(Liu and Wang, 2018), which can cause individuals to reduce sharing information publicly in general SNs (Hofstede, 2001). In work-oriented ESNs, however, relatively stable communication among colleagues can help avoid rich information misuse due to the implementation of real-name authentication and strict privacy policies (Li *et al.*, 2020; Karwatzki *et al.*, 2017). Sharing high-richness information publicly in ESNs can not only reduce uncertainty and equivocality (Daft and Lengel, 1986) but also narrow the imagination space (Lee *et al.*, 2019) and decrease misunderstandings and value conflicts (Xu *et al.*, 2011). The visibility of ESNs also helps to facilitate knowledge transfer and enhance users' online presence (Leonardi, 2015; Luo *et al.*, 2017). Overall, richer information in ESNs can be more effectively interpreted and understood (Fiesler *et al.*, 2017; Zhou *et al.*, 2021), and can stimulate public sharing. Accordingly, this study proposes:

H3. In the ESN context, information richness is positively related to users' public sharing. Specifically, the higher the information richness, the more likely users are to share information publicly.

3.3 Moderating effect of context-specific factors

Research has indicated that the pre-existing disposition to value information may be overridden by contextual factors in ESNs (Kehr *et al.*, 2013), as shown in this study. The disposition to value information is therefore presumed to interact with work-relatedness and information richness while acting on public sharing. Anderson and Agarwal (2011) proposed a CPM theory-based empirical model, hypothesizing that information sensitivity and privacy concerns affect the willingness to share health information. Their findings have suggested that compared to health information at the same sensitivity level, work-related information in ESNs is more sensitive, and its impact on public sharing is definitive (Fox and McEwan, 2017). Accordingly, it can be assumed that when the information shared is non-work-related, users' disposition to value information has a stronger negative effect on public sharing as the disposition to value information rises. A stronger negative effect on public sharing should exist for work-related information, while the negative effect of the disposition to value information on public sharing is diluted. That is, the negative effect of the disposition to value information on public sharing is weakened as work-relatedness increases. This study thus proposes:

H4. In the ESN context, work-relatedness negatively moderates the relationship between the

disposition to value information and public sharing. Specifically, the negative relationship between the disposition to value information and public sharing is mitigated when work-related information is shared, compared to non-work-related information.

Krämer and Haferkamp (2011) observed a conflict between providing rich information and the disposition to value information, which is seen as a barrier to sharing information publicly. After investigating privacy concerns and impression construction on SNs, they found that sharing rich information matches the goal of providing a detailed and accurate impression (Leonardi, 2015), but contradicts strategies to protect information privacy. According to MRT, rich information provides more means to communicate, including visual cues, compared to information with low richness (Zhou *et al.*, 2021). This stimulus makes users more likely to ignore the negative effects of pre-existing disposition to value information. That is, the disposition to value information plays a stronger negative role for information with relatively low richness, as low-richness information implies greater uncertainty and users are less likely to share it publicly to avoid potential misunderstandings and conflicts. Nevertheless, as information richness increases, the negative role of disposition to value information gradually decreases, and users are more likely to share information publicly. Therefore, the study predicts:

H5. In the ESN context, information richness negatively moderates the relationship between the disposition to value information and public sharing. Specifically, the negative relationship between the disposition to value information and public sharing diminishes as information richness increases.

3.4 Risk-benefit ratio and public sharing

CPM theory states that when users create or modify information boundaries, they weigh the benefits and risks (Laufer and Wolfe, 1977; Petronio, 1991). Such weighing, however, is subjective and potentially irrational (Min and Kim, 2015), as it can be intuitively or arbitrarily assigned by users (Acquisti and Grossklags, 2007). Public benefit awareness can enhance positive outcome beliefs and relationship-enhancing expectations of public sharing (Christofides *et al.*, 2009), which can be economic or social (Barth and de Jong, 2017). When public sharing is encouraged, users will likely maintain a positive self-concept, develop meaningful relationships, and gain a more accurate perception of real circumstances (Ellison *et al.*, 2011; Min and Kim, 2015). The public benefits

addressed in this study stem from social benefits that ESN users receive from public sharing, such as likes, comments, forwards, and favorites (Barth and de Jong, 2017), which represent others' affirmation of the shared information value (Li *et al.*, 2020). That is, users believe they have reaped considerable benefits from previous public sharing practices, spurring continued public sharing. Accordingly, this study infers:

H6. Public benefits of ESN users are positively related to public sharing. Specifically, the higher the public benefit, the more likely users are to share information publicly.

Public risks are psychological and functional threats involving the potential negative consequences of individuals losing control over sharing information (Xu *et al.*, 2012). Information privacy research has confirmed the importance of public risk in influencing information-sharing decisions (Dinev and Hart, 2006; Xu *et al.*, 2011), although subjective or irrational decision-making denoted in the privacy paradox may lead to biased perceptions of public risk (Barth and de Jong, 2017). If users face significant risk threats, they may adopt appropriate information control settings when sharing information (Cichy *et al.*, 2021; Ellison *et al.*, 2011). This study defines public risk in ESNs as the loss and severity of the negative consequences of public sharing (Cichy *et al.*, 2021; Dinev and Hart, 2006; Xu *et al.*, 2011). In this context, risk assessment is based on personal experiences related to privacy violations (Wisniewski *et al.*, 2015), where users showed concern about threats posed by active disclosure or unreasonable use of profile information (Chen, 2018; Cichy *et al.*, 2021; Laufer and Wolfe, 1977). Such threats evoke information-protective behaviors that affect public sharing behavior (Xu *et al.*, 2011). This study is not concerned with how to reduce public risks (Min and Kim, 2015), but looks at how employees use ESN information control settings to control information boundaries when faced with public risk threats. The study therefore assumes:

H7. Public risks of ESN users are negatively related to public sharing. Specifically, the higher the public risk, the less likely users are to share information publicly.

3.5 Control variables

Gender is also a factor influencing public sharing behavior (Lin and Armstrong, 2019; Liu and Wang, 2018, Zhang et al, 2019), and is thus included as a control variable in this study. The model also controls for age (Fiesler *et al.*, 2017; Schwartz-Chassidim *et al.*, 2020), the total amount of shared information (Schwartz-Chassidim *et al.*, 2020), and privacy experience (Xie *et al.*, 2014).

The total amount of shared information refers to the number of posts per ESN user, reflecting the intensity of use (Schwartz-Chassidim *et al.*, 2020). Privacy experience measures ESNs users' preferred information control settings (Xie *et al.*, 2014), where users are more likely to share publicly if they have previously engaged in public information sharing (Fiesler *et al.*, 2017; Habib *et al.*, 2019; Liu and Wang, 2018).

4. Variables and method

This study explores an ESN maintained by a software-as-a-service provider in China that services a private digital workspace for employee collaboration. Employees submit personal details including name, gender, and age to create an ESN profile and use different channels to share information. The study focuses on employees' information control behaviors for specific information.

4.1 Variables and measurement

This study used system logs to collect information-sharing data from ESN's wall posts channel. The data gathered from April 2013 to April 2018 recorded the attributes of 238 employees (e.g., name, age, and gender) and captured information attributes, including control settings, information content, information forms, and information disposal modules for 93,984 specific pieces of information shared by employees. Employee data and specific information data were cross-checked using MySQL, with mismatched data removed, leaving 93,281 specific information data nested as substructures in the records of 125 employees. Considering the business process perspective, this study removed the test data and data that was infrequently shared (i.e., less than 100 shared information pieces), leaving a total of 92,332 information data shared by 64 employees. Table I summarizes the employee demographics.

Table I. Employee demographics

Variable	Item	Frequency	Percentage (%)
Gender	Male	46	71.9
	Female	18	28.1
Age	<25	10	15.6
	25-29	30	46.9
	30-34	11	17.2
	35-40	6	9.4
	>40	7	10.9
The total amount of shared information (Toi)	100-500	30	46.9
	500-1000	11	17.2
	1000-2000	11	17.2
	2000-3000	5	7.8
	>3000	7	10.9
Privacy experience (Experience)	Mostly public (>80% public sharing)	0	0
	Mostly private (<20% public sharing)	47	73.4
	Other cases (20%-80% public sharing)	17	26.6

Note(s): The number of employees is 64. [1] Considering data across years, *Age* is categorized into five groups: under 25, 25-29, 30-34, 35-40, and 40+ years. [2] Based on Fiesler *et al.* (2017), there are only two types of *Privacy experience (Experience)* in this study: mostly private (<20% of information shared by the user is labeled as public sharing) and other cases (20%-80% public sharing). The results of the lower percentage of public sharing are in line with the findings of surveys (Hampton *et al.*, 2012) and large-scale analyses (Stutzman *et al.*, 2013).

Source(s): Author's own creation/work

Table II. Descriptive statistics of variables

Variable	Mean	Std. Dev.	Min	Max
Public sharing (Public)	0.197	0.397	0	1
The time order of information sharing (t)	2721.085	3640.240	1	16781
Disposition to value information (Disposition)	9.670	2.190	3	13
Work-relatedness (Work)	0.640	0.480	0	1
Information richness (Richness)	0.980	0.763	0	5
Public benefit (Benefit)	0.303	0.220	0	1
Public risk (Risk)	-0.059	0.864	-1.916	0.871

Source(s): Author's own creation/work

Table II yields descriptive statistics of variables, in which several aspects need clarification. First, this study uses t to record the time order in which ESN users shared each piece of information, e.g., $t = 1$ for the first time a user shared information, $t = 2$ for the second time, and so on.

Second, disposition to value information is the information disposal practice of ESN users that inherently protects the information boundary, which is measured by functional module usage (Schwartz-Chassidim *et al.*, 2020). Users who attach more importance to information value will consider the suitability of shared information and modules more carefully, leading to different information being disposed of in different modules (e.g., having a higher disposition to value information). The ESN contains 16 functional modules, including the general, task, file, and project modules, and Figure 3 shows information shared in the task module. Third, work-relatedness tagging is achieved by textual classification of information content using the model Enhanced Representation through kNowledge IntEgration (ERNIE). This study trains the ERNIE model with as much data and prior knowledge as possible, and the validation set accuracy is around 0.84 to 0.89. Fourth, information richness is expressed as the richness of the presentation of specific information (Fiesler *et al.*, 2017; Zhou *et al.*, 2021), measuring how many different forms are there for the specific information. ESNs have seven categories of information forms, including text, image, video, audio, link, document, and compressed file.

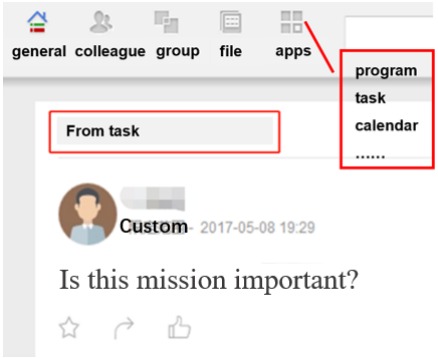

Figure 3. Example of functional module application in wall posts

Source(s): Author's own creation/work

Finally, public benefit is related to information-sharing response (Christofides *et al.*, 2009; Li *et al.*, 2020) as superimposed by the number of likes, comments, forwards, and favorites. Specifically, when user i determines whether the tth information is shared publicly, the public benefit $Benefit_{it}$ depends on the ratio of the total number of responses received by all publicly shared information before $t-1$ to the total number of responses received by all $t-1$ information. Public risk is assessed by the completeness of the user's profile, which in addition to basic information, includes phone number, education, career, interests, personality, blood type,

nation, address, and zip code. To measure public risk, this study treats these nine categories of information as dummy variables (Schwartz-Chassidim *et al.*, 2020) and uses a single-factor measurement model.

4.2 Research method

This study adopts the multilevel mixed-effects logistic regression method, meqrlogit, to test the hypotheses, as the data are multilayered and the dependent variable is a binary response that includes both fixed and random effects, making it suitable for modeling intra-cluster correlation. The fixed effects are specified as regression parameters and the random effects are the data structure grouping. The meqrlogit employs a QR decomposition of the variance component matrix, which helps converge as the variance components approach parameter space bounds. The estimation process involves a set of iterations that refine the initial values and a set of gradient-based iterations, with the default algorithm being the Newton-Raphson method.

Consider a logistic regression with the dependent variable Y_{it}, for a series of M independent users, conditioned on a set of random effects u_i, as shown in equation (1):

$$Pr(Y_{it} = 1|u_i) = \Phi(X_{it}\beta + Z_{it}u_i) \quad (1)$$

where t is a time index for $i = 1, \dots \dots, M$ users and each user i consists of $t = 1, \dots \dots, n_t$ observations, and Y_{it} is the dichotomous variable. The $1 \times p$ row vector X_{it} is the fixed-effect covariate with regression coefficient β, and the $1 \times q$ row vector Z_{it} is the corresponding random-effect covariate, denoting the random intercept and random coefficient. $\Phi(\cdot)$ is the logistic cumulative distribution function, $\Phi(v) = exp(v)/\{1 + exp(v)\}$.

Specifically, the dependent variable $Public$ is binary, and the key variables are $Disposition$, $Work$, $Richness$, $Benefit$, and $Risk$. This study considers a simple random intercept model with interaction effects and modifies it to have a random effect for each user i, per equation (2):

$$\begin{aligned} Pr\,(Public_{it} = 1) \\ &= \Phi(\beta_0 + \beta_1 Disposition_{it} + \beta_2 Work_{it} + \beta_3 Richness_{it} + \beta_4 Disposition_{it} \\ &* Work_{it} + \beta_5 Disposition_{it} * Richness_{it} + \beta_6 Benefit_{it} + \beta_7 Risk_{it} \\ &+ u_i) \quad (2) \end{aligned}$$

5. Results and discussion

5.1 Empirical results

The correlations between the variables were checked and the results revealed no significant multicollinearity, and the variance inflation factor values of the variables were all less than 10. To mitigate the latent multicollinearity in the cross-sectional terms of the moderating effects, this study borrowed the method from Balli and Sørensen (2012) to perform intra-cluster mean centralization. This helps avoid the spurious capture of different individual slopes in the ordinary interaction term regression.

Figure 4 shows the fixed effects results in the form of an odds ratio (OR). OR value greater than 1 implies that public sharing is more likely to occur than private sharing, and vice versa. The empirical results support most of the hypotheses. The direct effects of disposition to value information, work-relatedness, and information richness on public sharing were significant, confirming H1 to H3. The interaction effects between the disposition to value information and work-relatedness, and between the disposition to value information and information richness, were equally significant, supporting H4 and H5. As for H6, the results showed a significant positive effect of public benefits, but for H7, it was found to be insignificant, as the negative relationship between public risks and public sharing was not supported ($\beta = 0.945$, $p = 0.769$).

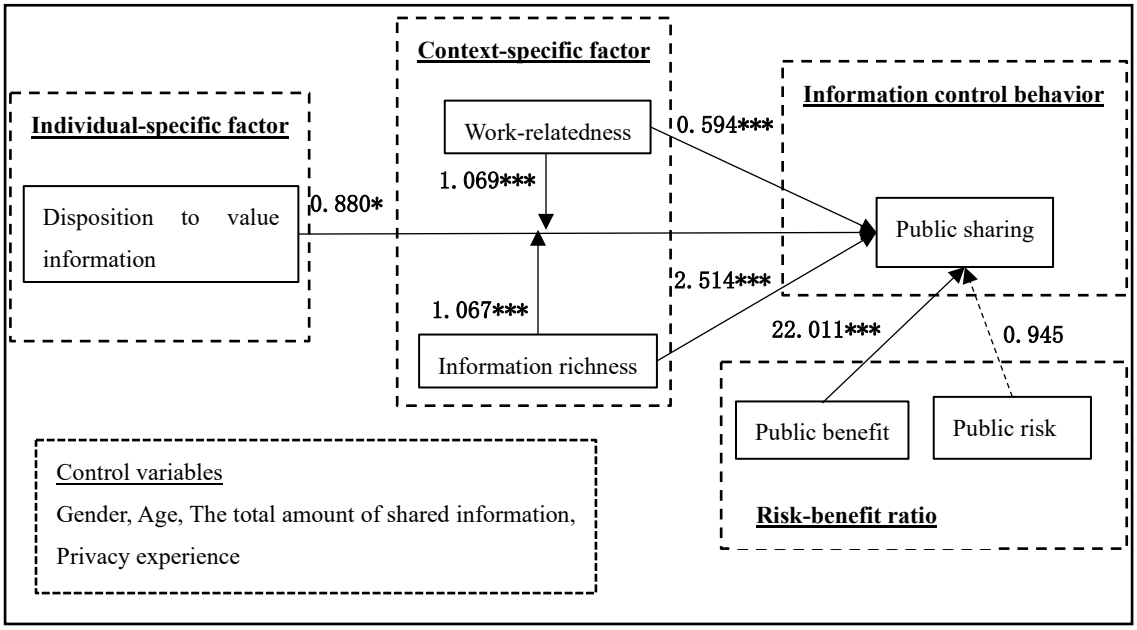

Figure 4. Empirical results

Note(s): *$p < 0.05$, **$p < 0.01$, ***$p < 0.001$. [1] The likelihood ratio test (LR chibar2(01) = 2980.05, p = 0.0000) showed that there was a significant difference between this model and the ordinary logistic regression ($u_i = 0$), and the intercept variation was not 0. The results suggest that individual differences are an important source of variation in public sharing, or that public sharing varies from person to person to a large extent. This in turn confirms the applicability of the layered model. [2] This study used standard logistic regression and estimated a model with constant terms only to report acceptable goodness of fit (Chen, 2014). The *pseudo-R^2* was calculated by comparing the log-likelihood of the two models: (38038.697-32655.151)/ 38038.697 = 0.142.

Source(s): Author's own creation/work

5.2 Further discussion

Some notable results warrant further discussion. First, the three direct hypotheses H1 to H3 are confirmed, with findings that are highly consistent with existing research. Results show that users with a higher disposition to value information in ESNs are wary of sharing information publicly. They inherently value their information boundaries (Xu *et al.*, 2011) and view others' minor use of information as highly invasive (Malhotra *et al.*, 2004). Furthermore, when it comes to work-related information, users will consider its potential professionalism (Liu and Kang, 2017) and sensitivity (Anderson and Agarwal, 2011) and tend not to share information publicly (Fox and McEwan, 2017). Additionally, ESNs users are more likely to share high-richness information publicly, just as MRT suggests that high-richness information reduces uncertainty and equivocality (Daft and Lengel, 1986) and helps avoid misuse, misunderstandings, and conflicts (Xu *et al.*, 2011; Karwatzki *et al.*, 2017).

Second, the model performs well in terms of interaction effects. Results show that both work-relatedness and information richness weaken the negative relationship between the disposition to value information and public sharing (H4 and H5), validating that information control should be adapted to contexts. The relationship between the disposition to value information and public sharing differs significantly for work-related and non-work-related information. Specifically, the negative effect of disposition to value information on public sharing is more pronounced for non-work-related information, where users' disposition to value information matters more. Importantly, there is a clear substitution between the disposition to value information and work-relatedness in influencing public sharing. Similarly, the role of disposition to value information varies significantly

across information richness levels. The negative effect of disposition to value information on public sharing is more pronounced at the low-richness level of information and mitigates as information richness increases. This suggests that the disposition to value information may also be important for low-richness information.

Finally, the desire for public benefits is found to stimulate public information sharing (Barth and de Jong, 2017; Ellison *et al.*, 2011), thus H6 is supported. Public risk has no significant influence, thus H7 does not hold. This outcome may be due to users' information privacy decisions that tend to ignore or underestimate risks, a phenomenon explained by the privacy paradox (Acquisti and Grossklags, 2004; Barth and de Jong, 2017). Under this premise, the impact of public risks on public sharing behaviors may be limited, an issue that warrants further investigation.

5.3 Robust extensions

In this study, the initial model (2) is a simple random intercept model containing only a user-level random effect u_i, which can be extended by the addition of the variable $Work$ to the random effects, per equation (3):

$$Pr\,(Public_{it} = 1) = \Phi(\beta_0 + \beta_1 Disposition_{it} + \beta_2 Work_{it} + \beta_3 Richness_{it} + \beta_4 Disposition_{it} * Work_{it} + \beta_5 Disposition_{it} * Richness_{it} + \beta_6 PBenefit_{it} + \beta_7 Risk_{it} + u_i + v_i Work_{it}) \quad (3)$$

The new model thus contains a random intercept and a random coefficient for $Work$, and allows for no correlation between the user-level random effects. The results are shown in model (3) in Table III, where the fixed effects remain largely stable. Model (3) is an improvement over the random intercept model (2), as confirmed by the results of the likelihood ratio test, the goodness of fit, and the AIC and BIC tests. To further optimize the model, this study relaxes the assumption of independence between random effects and assumes a correlation between u_i and v_i by specifying the covariance (unstructured) in the model, with the results of model (4) in Table III being consistently robust.

This study fits the data again using the generalized structural equation model (GSEM). Similar to meqrlogit, GSEM can fit a binary response mixed-effects model that includes both fixed and random effects and partially addresses the problem of omitted variables. The model output is shown

in model (5) in Table III, and the results remain robust. The study also re-runs the original model using 93,281 information data from 125 employees, both of which yield more consistent results.

Table III. Results of robustness tests

Model	*(1)* *Public*	*(2)* *Public*	*(3)* *Public*	*(4)* *Public*	*(5)* *Public*
Disposition	-0.0777	-0.127*	-0.164*	-0.165*	-0.0817***
	(0.0615)	(0.0624)	(0.0796)	(0.0787)	(0.00945)
Work	-0.499***	-0.521***	-0.757**	-0.724**	-0.505***
	(0.0238)	(0.0240)	(0.267)	(0.269)	(0.0226)
Richness	0.936***	0.922***	0.969***	0.970***	0.886***
	(0.0162)	(0.0163)	(0.0169)	(0.0169)	(0.0158)
Disposition * Work		0.0667***	0.232**	0.214*	0.0605***
		(0.0122)	(0.0880)	(0.0877)	(0.0112)
Disposition * Richness		0.0646***	0.0635***	0.0636***	0.0607***
		(0.00833)	(0.00861)	(0.00861)	(0.00793)
Benefit	3.103***	3.092***	3.162***	3.176***	3.468***
	(0.0862)	(0.0862)	(0.0894)	(0.0895)	(0.0792)
Risk	-0.0347	-0.0570	0.239	-0.0119	-0.256***
	(0.192)	(0.194)	(0.248)	(0.222)	(0.0195)
Gender	-0.370	-0.361	-0.615	-0.558	-0.139***
	(0.286)	(0.288)	(0.369)	(0.320)	(0.0318)
Age	-0.456***	-0.459***	-0.555***	-0.545***	-0.245***
	(0.0341)	(0.0341)	(0.0357)	(0.0357)	(0.0114)
Toi	0.0000868	0.0000896	0.0000576	0.0000905	0.0000436***
	(0.0000624)	(0.0000629)	(0.0000806)	(0.0000697)	(0.00000244)
Experience	2.721***	2.706***	2.262***	2.647***	2.341***
	(0.274)	(0.276)	(0.355)	(0.315)	(0.0251)
Constant	-2.958***	-2.946***	-2.799***	-2.920***	-2.659***
	(0.262)	(0.264)	(0.338)	(0.317)	(0.0248)
Log-likelihood	-32686.842	-32655.151	-31235.26	-31226.457	-34145.178
Likelihood-ratio test		63.38***	2839.78***	17.60***	
Pseudo-R^2	0.141	0.142	0.179	0.179	0.254
AIC	65395.68	65336.3	62498.52	62482.91	
BIC	65499.33	65458.79	62630.43	62624.25	

Note(s): *$p < 0.05$, **$p < 0.01$, ***$p < 0.001$. [1] Standard errors are in parentheses. [2] The regression method used for models (1) to (4) is meqrlogit, and model (5) uses GSEM. [3] The first part of Table III reports the coefficients (standard errors) and the significance levels of the fixed effects, and the second part reports the results of model comparisons. [4] The likelihood ratio test values for models (2), (3), and (4) respectively correspond to (1),

(2), and (3), indicating that the model is improving incrementally. [5] The *Pseudo-*R^2 of the model (5) is given based on the constant term model of GSEM: (45769.576-34145.178)/ 45769.576 = 0.254.

Source(s): Author's own creation/work

6. Conclusions

ESN users often neglect the use of the continuous information control settings employed during information sharing, although information control studies on the information disclosure intentions of users' profile pages found that they often express privacy concerns. This is especially the case in work-oriented ESNs, where users are more concerned with information control in broadcasting channels like wall posts and may consider all information as information privacy. This study highlights information privacy control as a crucial topic in ESNs (Keith *et al.*, 2014; Wang and Fussell, 2020), focusing on the wall posts and adapting CPM theory to elucidate information control behaviors and their key antecedents. The findings of actual behavioral data analysis show the direct effects of the individual-specific factor, context-specific factors, and risk-benefit ratio on employees' public sharing behaviors, emphasizing the interaction of individual motivational and contextual factors.

6.1 Theoretical implications

This study has three key theoretical contributions. First, it extracts the core maxim from the complex CPM framework: shared privacy boundaries. This provides a basis for normalizing CPM research by examining information boundaries in the ESN context and observing the consistency of information control and the shared privacy boundary of CPM theory. It also highlights the potential of information control as a new pathway to explain CPM theory and enhance its applicability. Importantly, information control should be more adaptive to context changes, where context-specific factors can act as moderators and interact with an individual-specific factor. This result not only confirms the interdependence of boundary rules in CPM theory and encourages researchers to re-conceptualize the relationships among boundary rules, but also creates a connection between CPM and MRT, providing insights for developing a more comprehensive theory of information control.

Second, this study focuses on information privacy in work scenarios and examines employees'

continuous information control behaviors in adapting to specific contexts, which expands the research boundary of information control behavior. Analysis of the moderating role of context-specific factors in ESNs reveals that information privacy constantly changes when adapting to specific contexts, as supported by the exclusive and positive role that information richness plays. The study thus fills the research gap in information control behavior in ESNs, and lays the foundation for extending information control research into new areas, thus developing unique understandings of information sharing.

Third, this study emphasizes the importance of incorporating actual information control behaviors data rather than reported sharing intentions, which exemplifies an objective way to validate users' true preferences and helps avoid the privacy paradox. User perception of the insignificance of public risk may corroborate this argument. That is, despite the strong relationship between weak information control attitudes and public risk, in actual information control behaviors, users tend to ignore or underestimate information risks.

6.2 Practical implications

The study also has three practical implications. First, the disposition to value information emphasizes the information disposal practices of ESN users, which are closely related to their familiarity with the ESN modules. The study, therefore, guides managers and developers to revisit ESNs' system tools, expand the information management functions of channels such as wall posts, rationalize information disposal modules, and strengthen training on the application of channels and modules so that employees can better adapt to and manage information control settings. Second, the findings can inspire employees to pay attention to contextual changes when dealing with information privacy in work scenarios. They also prompt managers to reasonably assign tasks, guide employees to manage information sharing in terms of work-relatedness and information richness, and help employees achieve effective business information control. Third, this study instructs managers to regulate employees' information privacy practices using actual behavioral data, without being subject to misinformation related to nebulous intentions or reported attitudes.

6.3 Limitations and future directions

This study has some limitations. Users' information control behaviors change over time, and

studies should explore more dynamic models of user behavior. This implies that researchers could continue to explore how often users update their information control settings and continuously assess information control behaviors longitudinally. Finally, studies can incorporate information control intentions into the model to further distinguish information control intentions and behaviors, and to enrich privacy paradox research.

References

Acquisti, A. and Grossklags, J. (2004), "Privacy attitudes and privacy behavior", Camp, L.J. & Lewis, S. (Ed.s), *Economics of Information Security, Advances in Information Security,* Springer, Boston, MA, pp. 165-178.

Acquisti, A. and Grossklags, J. (2007), "What can behavioral economics teach us about privacy?", Acquisti, A., Gritzalis, S., Lambrinoudakis, C., & di Vimercati, S. (Ed.s), *Digital Privacy*, Auerbach Publications, New York, pp. 363-377.

Anderson, C.L. and Agarwal, R. (2011), "The digitization of healthcare: boundary risks, emotion, and consumer willingness to disclose personal health information", *Information Systems Research,* Vol. 22 No. 3, pp. 469-490.

Ball, K., Daniel, E.M. and Stride, C. (2012), "Dimensions of employee privacy: an empirical study", *Information Technology & People,* Vol. 25 No. 4, pp. 376-394.

Balli, H.O. and Sørensen, B.E. (2012), "Interaction effects in econometrics", *Empirical Economics,* Vol. 45 No. 1, pp. 583-603.

Barth, S. and de Jong, M.D.T. (2017), "The privacy paradox – investigating discrepancies between expressed privacy concerns and actual online behavior – a systematic literature review", *Telematics and Informatics,* Vol. 34 No. 7, pp. 1038-1058.

Bassellier, G., Reich, B.H. and Benbasat, I. (2015), "Information technology competence of business managers: a definition and research model", *Journal of Management Information Systems,* Vol. 17 No. 4, pp. 159-182.

Bélanger, F. and James, T.L. (2020), "A theory of multilevel information privacy management for the digital era", *Information Systems Research,* Vol. 31 No. 2, pp. 510-536.

Campbell, A.J. (1997), "Relationship marketing in consumer markets: a comparison of managerial and consumer attitudes about information privacy", *Journal of Direct Marketing,* Vol. 11 No. 3, pp. 44-57.

Chen, H.-T. (2018), "Revisiting the privacy paradox on social media with an extended privacy calculus model: the effect of privacy concerns, privacy self-efficacy, and social capital on privacy management", *American Behavioral Scientist,* Vol. 62 No. 10, pp. 1392-1412.

Chen, J.V., Nguyen, H.V.V. and Ha, Q.-A. (2020), "Understanding location disclosure behaviour via social networks sites: a perspective of communication privacy management theory", *International Journal of Mobile Communications,* Vol. 18 No. 6, pp. 690-713.

Chen, Q. (2014), *Advanced Econometrics and Stata Applications* (in Chinese), Higher Education Press, Beijing.

Christofides, E., Muise, A. and Desmarais, S. (2009), "Information disclosure and control on Facebook: are they two sides of the same coin or two different processes?", *CyberPsychology & Behavior,*

Vol. 12 No. 3, pp. 341-345.

Cichy, P., Salge, T.O. and Kohli, R. (2021), "Privacy concerns and data sharing in the Internet of Things: mixed methods evidence from connected cars", *MIS Quarterly,* Vol. 45 No. 4, pp. 1863-1892.

Daft, R.L. and Lengel, R.H. (1986), "Organizational information requirements, media richness and structural design", *Management Science,* Vol. 32 No. 5, pp. 554-571.

Dinev, T. and Hart, P. (2006), "An extended privacy calculus model for E-Commerce transactions", *Information Systems Research,* Vol. 17 No. 1, pp. 61-80.

Duan, S.X. and Deng, H. (2022), "Exploring privacy paradox in contact tracing apps adoption", *Internet Research,* Vol. 32 No. 5, pp. 1725-1750.

Ellison, N.B., Vitak, J., Steinfield, C., Gray, R. and Lampe, C. (2011), "Negotiating privacy concerns and social capital needs in a Social Media environment", Trepte, S. & Reinecke, L. (Ed.s), *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web*, Springer, Berlin Heidelberg, pp. 19-32.

Endicott, S. (2021), "38 million records exposed, Microsoft Power Apps blamed", Windows Central, available at: https://www.windowscentral.com/microsoft-power-apps-expose-data-millions/ (accessed 3 August 2023)

Fiesler, C., Dye, M., Feuston, J.L., Hiruncharoenvate, C., Hutto, C.J., Morrison, S., Khanipour Roshan, P., Pavalanathan, U., Bruckman, A.S. and De Choudhury, M. (2017), "What (or who) is public? Privacy settings and social media content sharing", *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, *Portland OR,* Association for Computing Machinery, New York, NY, pp. 567-580.

Forsgren, E. and Byström, K. (2018), "Multiple social media in the workplace: contradictions and congruencies", *Information Systems Journal,* Vol. 28 No. 3, pp. 442-464.

Fox, J. and McEwan, B. (2017), "Distinguishing technologies for social interaction: the perceived social affordances of communication channels scale", *Communication Monographs,* Vol. 84 No. 3, pp. 298-318.

Golbeck, J. (2015), "Privacy controls", *Introduction to Social Media Investigation*, Syngress, Boston, MA, pp. 31-38.

Goswami, R. (2023), "Top 20 Enterprise Social Media Management Tools 2023", Statusbrew, available at: https://statusbrew.com/insights/enterprise-social-media-tools/ (accessed 3 August 2023)

Habib, H., Shah, N. and Vaish, R. (2019), "Impact of contextual factors on Snapchat public sharing", *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, *Glasgow, Scotland*, Association for Computing Machinery, New York, NY, pp. 1-13.

Hampton, K.N., Goulet, L.S., Marlow, C. and Rainie, L. (2012), "Why most Facebook users get more than they give", *Pew Internet & American Life Project*.

Hinde, C. and Ophoff, J. (2020), "The technological panopticon: electronic monitoring and surveillance within the workplace: employee turbulence through perceptions of privacy infringement", in Anthony, V. (Ed.), *Proceeding of 2020 Dewald Roode Workshop on Information Systems Security Research*, *Ames, IA, USA*, IFIP Working Group 8.11/11.13, p. 15.

Hofstede, G. (2001), *Culture's Consequences: Comparing Values, Behaviors, Institutions and Organizations Across Nations*, Sage Publications, Thousand Oaks, CA.

Karwatzki, S., Dytynko, O., Trenz, M. and Veit, D. (2017), "Beyond the personalization–privacy paradox: privacy valuation, transparency features, and service personalization", *Journal of Management Information Systems,* Vol. 34 No. 2, pp. 369-400.

Kehr, F., Wentzel, D. and Mayer, P. (2013), "Rethinking the privacy calculus: on the role of dispositional factors and affect", *Proceedings of the International Conference on Information Systems (ICIS 2013)*, *Milan, Italy*, AIS Association for Information Systems, Atlanta, GA, USA.

Keith, M.J., Maynes, C., Lowry, P.B. and Babb, J. (2014), "Privacy fatigue: the effect of privacy control complexity on consumer electronic information disclosure", in Myers, M.D. & Straub, D.W. (Ed.s), *Proceedings of the International Conference on Information Systems - Building a Better World through Information Systems (ICIS 2014), Auckland, New Zealand, December 14-17*, Association for Information Systems, Atlanta, GA, USA.

Krämer, N.C. and Haferkamp, N. (2011), "Online self-presentation: balancing privacy concerns and impression construction on social networking Sites", Trepte, S. & Reinecke, L. (Ed.s), *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web*, Springer, Berlin Heidelberg, pp. 127-141.

Laitinen, K. and Sivunen, A. (2020), "Enablers of and constraints on employees' information sharing on enterprise social media", *Information Technology & People,* Vol. 34 No. 2, pp. 642-665.

Laufer, R.S. and Wolfe, M. (1977), "Privacy as a concept and a social issue: a multidimensional developmental theory", *Journal of Social Issues,* Vol. 33 No. 3, pp. 22-42.

Lee, S.K., Kramer, M.W. and Guo, Y. (2019), "Social media affordances in entry-level employees' socialization: employee agency in the management of their professional impressions and vulnerability during early stages of socialization", *New Technology, Work and Employment,* Vol. 34 No. 3, pp. 244-261.

Leonardi, P.M. (2015), "Ambient awareness and knowledge acquisition: using social media to learn who knows what and who knows whom", *MIS Quarterly,* Vol. 39 No. 4, pp. 747-762.

Li, K., Cheng, L. and Teng, C.-I. (2020), "Voluntary sharing and mandatory provision: private information disclosure on social networking sites", *Information Processing & Management,* Vol. 57 No. 1, pp. 102-128.

Lin, S. and Armstrong, D. (2019), "Beyond information: the role of territory in privacy management behavior on Social Networking Sites", *Journal of the Association for Information Systems,* Vol. 20 No. 4, pp. 434-475.

Liu, B. and Kang, J. (2017), "Publicness and directedness: effects of social media affordances on attributions and social perceptions", *Computers in Human Behavior,* Vol. 75, pp. 70-80.

Liu, Z. and Wang, X. (2018), "How to regulate individuals' privacy boundaries on social network sites: a cross-cultural comparison", *Information & Management,* Vol. 55 No. 8, pp. 1005-1023.

Luo, J., Pan, X. and Zhu, X. (2017), "Discovery of repost patterns by topic analysis in enterprise social networking", *Aslib Journal of Information Management,* Vol. 69 No. 2, pp. 158-173.

Malhotra, N.K., Kim, S.S. and Agarwal, J. (2004), "Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model", *Information Systems Research,* Vol. 15 No. 4, pp. 336-355.

Min, J. and Kim, B. (2015), "How are people enticed to disclose personal information despite privacy concerns in social network sites? The calculus between benefit and cost", *Journal of the Association for Information Science and Technology,* Vol. 66 No. 4, pp. 839-857.

Petronio, S. (1991), "Communication boundary management: a theoretical model of managing disclosure of private information between marital couples", *Communication Theory,* Vol. 1 No. 4, pp. 311-335.

Petronio, S. (2002), *Boundaries of Privacy: Dialectics of Disclosure*, State University of New York Press,

New York, NY.

Petronio, S. and Durham, W.T. (2015), *Communication Privacy Management Theory*, John Wiley & Sons, Edison, NJ.

Pu, J., Chen, Y., Qiu, L. and Cheng, H.K. (2020), "Does identity disclosure help or hurt user content generation? Social presence, inhibition, and displacement effects", *Information Systems Research,* Vol. 31 No. 2, pp. 297-322.

Saraf, N., Langdon, C.S. and Gosain, S. (2007), "IS application capabilities and relational value in interfirm partnerships", *Information Systems Research,* Vol. 18 No. 3, pp. 320-339.

Schwartz-Chassidim, H., Ayalon, O., Mendel, T., Hirschprung, R. and Toch, E. (2020), "Selectivity in posting on social networks: the role of privacy concerns, social capital, and technical literacy", *Heliyon,* Vol. 6 No. 2, p. e03298.

Smith, H.J., Dinev, T. and Xu, H. (2011), "Information privacy research: an interdisciplinary review", *MIS Quarterly,* Vol. 35 No. 4, pp. 989-1015.

Smith, S.A. and Brunner, S.R. (2017), "To reveal or conceal: using communication privacy management theory to understand disclosures in the workplace", *Management Communication Quarterly,* Vol. 31 No. 3, pp. 429-446.

Stutzman, F., Gross, R. and Acquisti, A. (2013), "Silent listeners: the evolution of privacy and disclosure on Facebook", *Journal of Privacy and Confidentiality,* Vol. 4 No. 2, pp. 7-41.

Sun, Y., Fang, S. and Zhang, Z. (2021), "Impression management strategies on enterprise social media platforms: an affordance perspective", *International Journal of Information Management,* Vol. 60 No. C, p. 102359.

Venkatanathan, J., Kostakos, V., Karapanos, E. and Gonçalves, J. (2014), "Online disclosure of personally identifiable information with strangers: effects of public and private sharing", *Interacting with Computers,* Vol. 26 No. 6, pp. 614-626.

Vitak, J., Lampe, C., Gray, R. and Ellison, N. (2012), "Why won't you be my Facebook friend? Strategies for managing context collapse in the workplace", *iConference 2012, Toronto, Ontario, Canada*, Association for Computing Machinery, New York, NY, USA, pp. 555-557.

Wang, C.A., Karahanna, E. and Xu, Y. (2022), "Peer privacy concerns: conceptualization and measurement", *MIS Quarterly,* Vol. 46 No. 1, pp. 491-530.

Wang, L. and Fussell, S.R. (2020), "More than a click: exploring college students' decision-making processes in online news sharing", Vol. 4 No. GROUP, *Proceedings of the ACM on Human-Computer Interaction*, *New York, NY, USA*, Association for Computing Machinery, New York, NY, pp. 1-20.

Wang, Y., Zheng, D., Huang, L. and Huang, L. (2019), "The connotation, characteristics and research trend of enterprise social media" (in Chinese), *Science and Technology Management Research,* Vol. 39 No. 1, pp. 256-265.

Wisniewski, P., Jia, H., Xu, H., Rosson, M.B. and Carroll, J.M. (2015), "Risk-taking as a learning process for shaping teen's online information privacy behaviors", *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing*, *Vancouver BC, Canada*, Association for Computing Machinery, New York, NY, USA, pp. 583-599.

Xie, J., Knijnenburg, B.P. and Jin, H. (2014), "Location sharing privacy preference", *Proceedings of the 19th International Conference on Intelligent User Interfaces*, *Haifa Israel*, Association for Computing Machinery, New York, NY, USA, pp. 189-198.

Xu, H., Dinev, T., Smith, J. and Hart, P. (2011), "Information privacy concerns: linking individual

perceptions with institutional privacy assurances", *Journal of the Association for Information Systems,* Vol. 12 No. 12, pp. 798-824.

Xu, H., Teo, H.-H., Tan, B.C.Y. and Agarwal, R. (2012), "Research note – Effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: a study of location-based services", *Information Systems Research,* Vol. 23 No. 4, pp. 1342-1363.

Yang, X., Ye, H. and Wang, X. (2021), "Social media use and work efficiency: insights from the theory of communication visibility", *Information & Management,* Vol. 58 No. 4, p. 103462.

Yee, R.W.Y., Miquel-Romero, M.-J. and Cruz-Ros, S. (2021), "Why and how to use enterprise social media platforms: the employee's perspective", *Journal of Business Research,* Vol. 137 No. C, pp. 517-526.

Zhang, X., Ma, L., Xu, B. and Xu, F. (2019), "How social media usage affects employees' job satisfaction and turnover intention: an empirical study in China", *Information & Management,* Vol. 56 No. 6, pp. 103-136.

Zhou, C., Li, K. and Lu, Y. (2021), "Linguistic characteristics and the dissemination of misinformation in social media: the moderating effect of information richness", *Information Processing & Management,* Vol. 58 No. 6. p. 102679.

Zhou, Q., Li, H. and Li, B. (2023), "Employee posts on personal social media: the mediation role of work-life conflict on employee engagement", *Current Psychology,* Vol. ahead-of-print No. ahead-of-print.