SNS use reduction: a two-facet privacy concern perspective

Joana Neves (NOVA Information Management School (NOVA IMS), Universidade Nova de Lisboa, Campus de Campolide, Lisboa, Portugal)

Ofir Turel (School of Computing and Information Systems, The University of Melbourne, Melbourne, Australia)

Tiago Oliveira (NOVA Information Management School (NOVA IMS), Universidade Nova de Lisboa, Campus de Campolide, Lisboa, Portugal)

This is the accepted author *manuscript of the following article published by EMERALD:*
Neves, J., Turel, O., & Oliveira, T. (2022). SNS use reduction: a two-facet privacy concern perspective. Internet Research. https://doi.org/10.1108/INTR-01-2022-0012

Funding: This work was supported by national funds through FCT (Fundação para a Ciência e a Tecnologia), under the project –UIDB/04152/2020 – Centro de Investigação em Gestão de Informação (MagIC)/NOVA IMS.

emerald PUBLISHING

Internet Re

SNS use reduction: A two-facet privacy concern perspective

Journal:	*Internet Research*
Manuscript ID	INTR-01-2022-0012.R3
Manuscript Type:	Research Paper
Keywords:	Social networks, Privacy, Behaviour

SNS use reduction: A two-facet privacy concern perspective

Please find below the responses and summary of changes we made to address the concerns expressed.

Internet Research Editorial Office

Internet Research Editorial Office comment: Your manuscript, INTR-01-2022-0012.R3, entitled "SNS use reduction: A two-facet privacy concern perspective" has been unsubmitted to Internet Research. It may either have been rescinded.

It is because the manuscript has room for improvement before it can be accepted for publication. There are some typos (e.g., "institutional privacy concern have a broader effect", "institutional privacy concern reduce the level of engagement and information disclosure", "institutional privacy concern reflect and signal lower control"). Employing a professional copy-editing service is recommended.

Please revise the manuscript thoroughly and submit it again. Thank you.

Authors comment: Thank you for your suggestion. We used a professional copy-editing service to improve the readability of our paper and correct some grammar mistakes, including the ones referred. We did our best to identify all typos.

SNS use reduction: A two-facet privacy concern perspective

Abstract

Purpose: While social networking sites (SNS) have many positive aspects, they can have several adverse outcomes, among which privacy violations are a vital concern. We first posit that concerns regarding privacy violations can drive attempts to reduce SNS use. Next, we note that these violations can have two sources: peers and the social media provider. Thus, there is a need to understand how this complex system of privacy concerns affects use reduction decisions. To do so, this paper aims to examine the separate and joint roles of *institutional* and *peer* privacy concerns in driving SNS use reduction.

Design/methodology/approach: Based on privacy calculus theory, we propose a theoretical model to explain SNS use reduction, with *institutional* and *peer* privacy concerns as independent variables. The authors empirically examine the research model using a sample of 258 SNS users.

Findings: This study reveals that institutional and peer privacy concerns independently increase one's intention to reduce SNS use and that institutional privacy concern strengthen the relation between peer privacy concern and the intention to reduce SNS use.

Originality: Research thus far has not examined how the two facets of privacy work in tandem to affect 'users' decisions to change their behaviors on SNS platforms. Considering the unique and joint effect of these facets can thus provide a more precise and realistic perspective. This paper informs theories and models of privacy and online user behavior change.

Keywords: social networking sites (SNS), use reduction, peer privacy concern, institutional privacy concern, user behavior

SNS use reduction: A two-facet privacy concern perspective

1. Introduction

Social networking sites (SNS) allow sharing and reading of textual and visual posts and connecting with others. They have become a commonly used tool connecting individuals and companies without geographical limits or time constraints. For instance, Facebook has more than 2 billion daily users (about 30% of the world's population) (Vaghefi *et al.*, 2020). Despite their many benefits, recent studies suggest that social media platforms can adversely affect users, including problematic and excessive use (Turel and Qahri-Saremi, 2016), fatigue, distraction, and stress (Tarafdar *et al.*, 2020). Such negative consequences have led many users to quit (Cho, 2015; Turel, 2015; York and Turcotte, 2015) or to at least try to reduce their SNS use (Osatuyi and Turel, 2020). Motivators of SNS use reduction include fatigue, overload, and techno-stress (Maier *et al.*, 2015). Specifically, we posit that changing one's behavior on SNS can also, beyond the known factors, be motivated by privacy concerns. This hypothesis is rooted in the idea that privacy is something that people care about, and that people will change their behavior or pick behaviors to ensure their private information is protected (Dinev and Hart, 2003; Hong and Thong, 2013; Malhotra *et al.*, 2004). Such concerns exist and may be accentuated on SNS platforms (Choi and Land, 2016) because SNS platforms allow the collection of personal information on a big scale, raising users' and the public's concerns about privacy (Ozdemir *et al.*, 2017).

Because privacy concerns on social media are multifaceted and complex, our focus on privacy concerns as motivators of SNS use reduction enriches research in this domain. It highlights new opportunities for research on privacy concerns online. Specifically, the majority of extant studies on online privacy concerns have typically focused on concerns that the platform, website, or organization behind them will exploit the data (Bansal *et al.*, 2016; Cheng *et al.*, 2021; Ozdemir *et al.*, 2017; Wang and Herrando, 2019; Yu *et al.*, 2020). This facet of privacy concern is called *institutional privacy concern*. However, that is an incomplete point of view since, with the use of

SNS, peers are also a source of privacy threat and loss; they can take one's information and share it without permission. This facet of concern is called *peer privacy concern* (Ozdemir *et al.*, 2017). Research thus far has not examined how these two facets work in tandem to affect users' decisions to change their behaviors on SNS platforms. Considering the unique and joint effects of these facets can thus provide a more precise and realistic picture of reality. We hence seek to address this gap with the hope that this informs theories and models of privacy and online user behavior change and provides essential practical insights.

Overall, our study fills three gaps in the literature. First, the need to identify more theory-based drivers of use reduction as a way to correct SNS use behavior. Second, the need to study how privacy concerns might drive SNS corrective behaviors. Finally, the need to examine the effect of both facets of privacy concern (institutional and peer) and their interrelation on SNS users' behavior to study this two-facet privacy concern view in other IS use domains. Thus, the main research questions we aim to address are: (1) Can privacy concerns motivate intended SNS use reduction? ; (2) How do the two facets of privacy concerns work in tandem to impact SNS use reduction?

To understand the intricate association between privacy concerns and use reduction on SNS platforms, we theorized a model and tested it with a sample of 258 Instagram users. The findings show that institutional and peer privacy concerns motivate intended use reduction (unique effects), and institutional privacy concern moderates the effect of peer privacy concerns on intended use reduction (jointly dependent effect). Thus, considering the simultaneous effects of both facets presents a broader perspective than before on the role of institutional privacy concern in motivating user behavior.

Consequently, our study makes four key contributions. First, it extends research by considering a more nuanced and realistic perspective of privacy concerns. As we show, at least in the SNS use context, it includes two facets: institutional and peer concerns. We hope this conclusion might be helpful for other theories and privacy models, especially in online use behavior. Second, it shows that focusing only on one of these two facets of privacy depicts a partial picture, as both facets and their interaction affect use reduction intentions; that is, the effect of one is contingent on the

level of the other. This means it is essential to consider the peers' threat to privacy and not only the SNS provider threats since there is a significant interaction effect between the two facets that strengthens the intention to reduce SNS use. Each facet alone does not capture the whole effect of privacy concerns. Including both facets has an extra tandem effect on reduction intentions is essential. Third, it discovers the motivational potency of two facets of privacy concerns in driving intended SNS use reduction. This highlights the power of privacy considerations in motivating corrective behaviors on SNS. Lastly, the results can serve as a basis for interventions to help social media platforms to better cater to 'users' privacy needs and expectations. We do all this while exploring more profound and essential yet primarily ignored behavior - SNS use reduction, which merits further research (Osatuyi and Turel, 2020; Soliman and Rinta-Kahila, 2020).

The rest of the paper is structured as follows. Section 2 provides the theoretical background about SNS corrective behaviors and privacy concerns. Section 3 outlines the research model and hypotheses. Section 4 presents the methodology used and describes the data. Section 5 contains the data analysis and results. Section 6 offers a discussion of the results, as well as some limitations and future research directions. Finally, Section 7 provides the conclusion of the work.

2. Theoretical Background

2.1. SNS use reduction

When an individual faces actual or potential negative consequences stemming from the use of SNS, they are motivated to take corrective behaviors aimed at reducing or eliminating the actual or potential adverse effects (Osatuyi and Turel, 2020). Common corrective behaviors include quitting, temporary discontinuance, and reduction behaviors. Quitting is an aggressive attempt to curtail one's problems (Osatuyi and Turel, 2020), as it eliminates the source of the problem (Luqman *et al.*, 2018; Turel, 2014; Vaghefi and Qahri-Saremi, 2017). However, it is taxing because it also eliminates all the benefits the IS can provide. Taking a temporary break from using a system represents a similar approach, though it allows for a quick solution; one's problems will likely persist after resuming the system. Nevertheless, it is more realistic and practical than entirely quitting system use (Ravindran *et al.*, 2014; York and Turcotte, 2015). Lastly, use

reduction is a less aggressive approach, which seems more doable compared to the abovementioned approaches; it is thus a more realistic long-term solution that many (and certainly not all) users adopt to address actual or potential problems associated with SNS use (Osatuyi and Turel, 2020). It reflects attempts to decrease the use of the SNS to levels with which one can still feel comfortable, but that also reduces the potential for problems. Entirely quitting SNS use is the most studied corrective behavior on SNS. The other two approaches, taking a break from use and use reduction, received much less attention in the extant literature, despite the lower realism and attractiveness of entirely quitting social media (Osatuyi and Turel, 2020; Ravindran *et al.*, 2014).

Notably, for our study, known predictors of use reduction include addiction, peer use reduction, and the realization that one's use pattern is problematic and deviates from their expectations (Osatuyi and Turel, 2020). SNS fatigue is the most commonly used driver to explain discontinuance (Fu and Li, 2020; Niu *et al.*, 2020; Ravindran *et al.*, 2014; Shokouhyar *et al.*, 2018). Even though very few studies have focused on understanding SNS use reduction. Table I shows some of the most important ones and the drivers they explored. Our review suggests that existing models overlook or oversimplify the potential role of privacy concerns in motivating corrective behaviors, despite the natural tendency of humans to pursue behaviors that will protect and retain their privacy (Dinev and Hart, 2003; Hong and Thong, 2013; Malhotra *et al.*, 2004). Overall, we conclude that despite the prevalence, potential, and importance of use reduction, it did not receive sufficient attention, and there is potential to extend our understanding of the drivers of this behavior by considering the privacy angle. We aim to address these two gaps in the current study.

Specifically, among the few studies that focused on use reduction, insufficient emphasis has been given to a significant concern on social media, namely regarding one's privacy. This is a common concern that motivates various behaviors on social media, as it is integrated into the decision calculus of social media users (Chen, 2018; Gruzd and Hernández-García, 2018; Jozani *et al.*, 2020). Thus, we theoretically develop an argument that it can also influence decisions to reduce one's use of social media.

Source	Theory/framework	Drivers	Outcome
Islam *et al.* (2022)	Lazarus and Folkman's theory of stress and coping	Global pandemic Stressors, COVID-19 obsession, Emotional support seeking through SNS, SNS exhaustion	SNS reduction intentions
Osatuyi and Turel (2020)	Social identity theory, Social cognitive theory	SNS addiction, Realization, Peer reduction of SNS use	SNS reduction intentions
Shokouhyar *et al.* (2018)	-	Information overload, System feature overload, Social overload, SNS fatigue	Controlled SNS activities*
Niu *et al.* (2020)	Stimulus-Organism-Response	Information overload, Negative social comparison, SNS fatigue	SNS reduction intentions
(Fu and Li (2020)	Social cognitive theory	Technology overload, Information overload, Social overload, SNS fatigue, Dissatisfaction	Reduced usage behavior
Ravindran *et al.* (2014)	-	Platform-related factors, Community-related factors (social dynamics, content, life cycle), Factors relating to self (immersive, tendencies), Individual experiences resulting in negative emotions	Controlled SNS activities*

Table I. Summary of SNS use reduction studies

* The SNS activities are performed in a controlled way, namely in terms of use duration. Very similar to use reduction in the sense that it is measured by asking the intentions to use less SNS than today

2.2. Privacy concerns

Privacy concerns are considered in 'users' mental calculus, given the massive amount of personal information that is in digital format that can be easily collected, stored, copied, and used by others (Choi *et al.*, 2018; Hong and Thong, 2013; Malhotra *et al.*, 2004). The prevalence and magnitude of SNS use give rise to new privacy-related challenges. Users can see their information exposed on the internet and realize that they have lost control over their information: they have no way, in many cases, to know who it is shared with, for what purposes, and if it was shared beyond the initial post (Bright *et al.*, 2015; Choi *et al.*, 2018).

At the elementary level, users need to trust the SNS provider to agree to share their personal information on the platform. This is because users become vulnerable when they post personal information (Ayaburi and Treku, 2020). However, privacy breaches by SNS (e.g., Cambridge Analytica and Facebook scandal in 2018, used the information about 50 million users as a way to identify the personalities of the American voters and manipulate their behavior ("Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens", 2018)) have ignited concerns

in many users regarding the way their private information is handled, thereby creating an increased privacy concern on social media (Ayaburi and Treku, 2020; Zhou and Li, 2014). This is because the majority of users expect to have control over the information they share (Kuenzler, 2022), which some studies refer to as the "personal information sphere" (Eskens, 2020). However, this does not typically happen, and many users see their private information exposed in unexpected ways.

Research on privacy in the SNS use context is, to some extent, contradictory. Even when users say they care about their privacy, at the same time, they do not act to protect their information; this is known as the privacy paradox (Chen, 2018). Other scholars affirm that people who care about their privacy change their behavior to ensure that their information is kept private, following the privacy calculus theory (Cain and Imre, 2021; Jiang *et al.*, 2013). As such, there is a need for more research in this area. Thus, this study will also try to evaluate the role of privacy concerns in motivating corrective behavior on SNS.

The privacy calculus theory suggests that when users experience a violation of their privacy, they will respond with a privacy-seeking behavior using strategies such as refusal, complaining, or disengagement (Adjerid *et al.*, 2018; Ayaburi and Treku, 2020). The theory of planned behavior (TPB) (Ajzen, 2012) can also explain user responses (e.g., discontinuance intentions) to technology that threatens people's privacy expectations and desires (Yu *et al.*, 2020). The third lens of analysis used in this domain is the communication privacy management theory. It explains the process of self-disclosure. When users decide to disclose information online, they weigh costs vs. benefits, and the balance determines what information should be considered public vs. private (Chennamaneni and Taneja, 2015). From this perspective, users create boundaries to determine the contexts and circumstances that specific information should be disclosed (Morlok, 2016). As such, individuals expect that information disclosed will be protected such that their privacy expectations are met. When those boundaries are breached or are expected to be breached, for example, through privacy violations, individuals attempt to seek a way to solve the situation and mitigate the problem (Xu *et al.*, 2011).

One way to cope with privacy concerns, which users at least often contemplate, is behavior change on the platform that concerns them (Cheng *et al.*, 2021; Wang and Herrando, 2019). Indeed, privacy concerns negatively impact 'users' intention to use or continue using a specific SNS (Ayaburi and Treku, 2020; Cain and Imre, 2021; Desimpelaere *et al.*, 2020; Dhir *et al.*, 2019). This is because users who feel that their data privacy expectations may not be met will likely take measures to mitigate the problem; this can be achieved partly by altering their use pattern (Choi et al., 2018; Zhang et al., 2020). For example, discontinuance will eliminate privacy concerns regarding new information one can share. In contrast, the risk of SNS uses reduction decreases (but does not eliminate). Because social media use often involves sharing information. Even when it is not done explicitly (e.g., when people do not post), there is implicit information sharing on one's activities online (e.g., login location, device, browsing history) (Ruths and Pfeffer, 2014), reducing one's use is a reasonable strategy for alleviating privacy risks and consequent concerns. It is a compromise that affords reducing privacy risks but maintains SNS benefits. In contrast, full discontinuance will eliminate the risk, but for many people, it will not afford normal social functioning (Osatuyi and Turel, 2020).

Without discounting the importance and impact of this line of work, one of its limitations is that most of the studies on privacy concerns have focused on understanding intentions to disclose personal information as an outcome. Few studies have focused on the ability of privacy concerns to motivate behavior change, especially in the form of use reduction (as opposed to total discontinuance). Another limitation of extant works on privacy on SNS is that they have focused mainly on the institutional perspective of privacy concerns (Cheng *et al.*, 2021; Yu *et al.*, 2020). This is an overly simplistic view because privacy threats on SNS can stem from the institutions (the social media platforms) and the users (i.e., peers who have access to at least some aspects of one's information). Moreover, as we theorize in the next section, one concern can moderate the effect of the other. Thus, commonly observed effects of single-facet privacy concerns might be contingent on the levels of the other privacy concern facet. Ultimately, there is a need to focus on the two facets of privacy concerns (institutional and peer) because this can depict a more nuanced

and precise picture regarding how privacy concerns motivate behavior change on SNS. Here, we seek to make first strides toward bridging these gaps.

To this end, we note that privacy concerns do not only relate to or stem from sharing information with the SNS organizations but can also relate to or stem from sharing information with peers on social media (Jozani *et al.*, 2020; Ozdemir *et al.*, 2017). This distinction has been highlighted in recent studies pointing to two facets of privacy concerns: institutional privacy concern, related to the misuse of personal data entrusted to an institution, and peer privacy concern, associated with the misuse of personal data entrusted to peers of an individual (Raynes-Goldie, 2010). Extending these works, we suggest that both perspectives need to be included in studies about SNS use reduction because when a user shares something on the SNS, that information becomes co-owned. The risk of what peers can do with the data they are given access to is higher (Ozdemir *et al.*, 2017). Examples of possible misuse of personal information by peers can be when someone tags photos of a user on Instagram or Facebook without consent or identifying a user on Instagram stories showing where they are and what they are doing without permission when peers post something on a user's Facebook profile without consent, or when peers use the user's data inappropriately accessed through SNS (Chen *et al.*, 2015; Marwick and Ellison, 2012; Ozdemir *et al.*, 2017; Vitak, 2012).

Such behaviors can drive peer privacy concern and are not captured by the often-studied institutional privacy concern. How peers use the user's private information also influences how users might share information and SNS use levels. Following the work of Hogan (2010), users may deal with a context collapse by sharing the appropriate information according to the peers that can access that information. The information transmitted must be suitable for all peers to see (the closest ones and the others) without putting the users at risk. Therefore, SNS use levels can be influenced by institutional privacy concern and peer privacy concern. We posit and later show that moving forward, there is merit to including both privacy concern facets in information systems studies, also because the effect of one is contingent on the other.

3. Research model and hypotheses

Figure 1 shows the proposed research model. It hypothesizes that peer privacy and institutional privacy concerns motivate (increase) one's intention to reduce SNS use. It further suggests that institutional privacy concern has a broader effect on behavior change: not only do they motivate behavior change directly, but also, they increase the emphasis on peer privacy concern in users' privacy calculus leading to adjusting one's behavior on the SNS. Next, the justification for the hypotheses in the research model is provided.

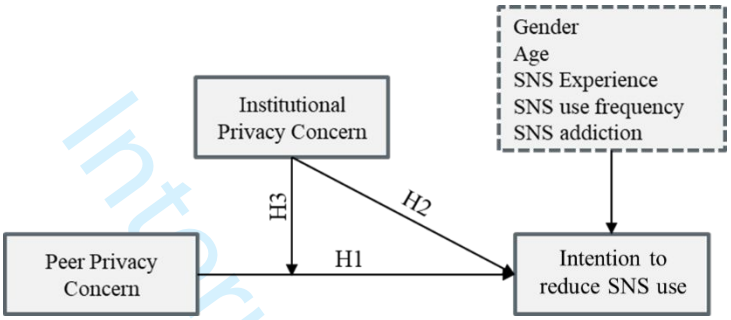

Figure 1- Research model

3.1. Effects of Peer Privacy Concern

Peer privacy concern captures worries related to the possible misuse of personal data entrusted to an individual's peers (Raynes-Goldie, 2010). For example, peers can share personal correspondence (pictures, text, emotions, insights) on social media that was intended only for them. Like other concerns, worries regarding peers violating one's privacy expectations, as manifested in higher levels of peer privacy concern, drive users to respond with a mitigation behavior, including avoiding SNS use or reducing one's exposure to SNS ((Ozdemir *et al.*, 2017). As such, users concerned with peers violating their privacy expectations will likely try to reduce their interaction with their peers to a level that will allow them to still communicate with them, but that will also put their privacy risk exposure at an acceptable level to them. Thus, users will likely perceive use reduction as a practical compromise approach that allows them to retain social ties but still reduce privacy violation risks (Ozdemir *et al.*, 2017). We therefore hypothesize:

H1: Peer privacy concern will increase one's intention to reduce SNS use.

3.2. Effects of Institutional Privacy Concern

The level of concern that the users have about the misuse of their personal information by SNS organizations is another essential motivator of use reduction in the SNS use context. Similar to the argument behind H1, we posit that one reasonable response to such concerns would be use reduction. This compromise approach allows users to maintain social ties online (this would not be afforded with total discontinuance) but controls (or reduces) their risk exposure. The risk exposure is diminished because use reduction will result in fewer data collected about the user by the SNS provider, reducing the opportunity for information misuse (Zhang et al., 2020). Indeed, institutional privacy concern reduces the level of engagement and information disclosure on SNS (Dhir *et al.*, 2019; Jozani *et al.*, 2020; Zhou and Li, 2014). Here, we suggest that a "compromise" corrective behavior in the form of use reduction (Osatuyi and Turel, 2020) is a reasonable response to privacy calculus beliefs about risks, including those stemming from the potential misuse of one's information by the SNS provider (Lin *et al.*, 2020; Wang *et al.*, 2021). Thus, we hypothesize:

H2: Institutional privacy concern will increase one's intention to reduce SNS use.

We next posit that the two facets of privacy concerns may act in tandem to drive intended use reduction. We specifically suggest synergy between them. The effect is more than the mere sum of the facets when both exist. The reason is that institutional privacy concern reflects lower control of the SNS provider over information handling matters and lower motivation to control internal (institutional) and external (peer) privacy threats (Kehr *et al.*, 2015; Lutz and Ranzini, 2017). Such lower care about privacy matters can attenuate the impact of privacy concerns on user responses (Taylor *et al.*, 2009). This is akin to the trust transfer process: trustworthy websites signal their users are reliable (Stewart, 2003). The difference is that here we hypothesize on "privacy concern transfer" from the SNS provider to peers on the SNS.

Specifically, we expect that when institutional privacy concerns are low, people perceive higher assurances that the SNS is competent and motivated to preserve their privacy. In this case,

concerns about privacy violations by peers may be less influential in the privacy calculus. That is, they may believe that the SNS provider can and is willing to protect them against privacy violations by peers. In contrast, when the value of institutional privacy concern is high, the prevailing perception would be that the users are on their own and no one will help them or protect them against privacy violations by peers. Consequently, we posit that institutional privacy concern moderates the effect of peer privacy concern on SNS use reduction and not the other way around. This is because, following the "privacy concern transfer process" described above, the organization typically shields against privacy concerns related to users and not the other way around. The reverse is usually unlikely—peers often have no control over the service and its privacy policies. As such, we expect that:

H3: Institutional privacy concern will moderate (increase) the effect of peer privacy concern on one's intention to reduce SNS use.

4. Methods

4.1. Measurement

Items were adapted from validated scales to the context of Instagram. We focus on Instagram, given its popularity and potential to drive privacy concerns (Liang *et al.*, 2015; Ranzini *et al.*, 2020; Shane-Simpson *et al.*, 2018). The items were included in an online questionnaire after pilot testing with 50 Instagram users. The pilot test corrected some linguistic mistakes, and some of the questions (socio-demographic) were reorganized. See Table II. In line with prior studies, we controlled for age, gender (Osatuyi and Turel, 2020), use frequency, SNS use time per day (minutes), SNS experience (years using SNS) (Vaghefi *et al.*, 2020), and SNS addiction (Turel and Qahri-Saremi, 2016b), because these may impact one's intention to reduce the SNS use.

Construct	Items	Sources
Peer privacy concern (PPC)	PPC1: I am concerned that the information I share through Instagram with people I know could be misused by them. PPC2: I am concerned about sharing information through Instagram with people I know, because of what they might do with it. PPC3: I am concerned about sharing information through Instagram with people I know because they could use it in a way I did not foresee. PPC4: I am concerned that when I share information through Instagram with people that I know, those people may share it with others whom I did not intend.	(Ozdemir et al., 2017)

		PPC5: I am concerned that the information I share through Instagram with people I know could be misinterpreted by them.	
Institutional privacy concern (IPC)		IPC1: I am concerned that the information I share through Instagram could be misused by Instagram and 3rd party affiliates. IPC2: I am concerned about sharing information through Instagram, because of what Instagram and 3rd party affiliates might do with it. IPC3: I am concerned about sharing information through Instagram, because Instagram and 3rd party affiliates could use it in a way I did not foresee. IPC4: I am concerned that when I share information through Instagram, they and 3rd party affiliates may share it with others whom I did not intend. IPC5: I am concerned that the information I share through Instagram could be misinterpreted by Instagram and 3rd party affiliates	(Ozdemir et al., 2017)
SNS addiction (ADD)	Social effect (SE)	SE1: How often do your grades or schoolwork suffer because of the amount of time you spend on Instagram? SE2: How often do you snap, yell, or act annoyed if someone bothers you while you are on Instagram? SE3: How often do you try to hide how long you've been on Instagram? SE4: How often do you choose to spend more time on Instagram over going out with others? SE5: How often do you feel depressed, moody or nervous when you are not on Instagram, which goes away once you are back on Instagram? SE6: How often do you try to cut down the amount of time you spend on Instagram and fail? SE7: How often do you check your Instagram before something else that you need to do? SE8: How often do you block out disturbing thoughts about your life with soothing thoughts of Instagram?	(Kircaburun and Griffiths, 2018)
	Compulsion (COM)	COMP1: How often do you find yourself anticipating when you will go on Instagram again? COMP2: How often do you fear that life without Instagram would be boring, empty, and joyless? COMP3: How often do you lose sleep due to late night logins to Instagram? COMP4: How often do you find yourself saying just a few more minutes" when on Instagram?	
Intention to reduce SNS use (RED)		RED1: I intend to reduce using Instagram in the next 3 months. RED2: I predict I would reduce using Instagram in the next 3 months. RED3: I plan to reduce using Instagram in the next 3 months.	(Osatuyi and Turel, 2020)

Table II. Measurement instrument

4.2. Procedure Sample

We created an online survey in English. It was distributed via a class announcement to a group of university students in Portugal. Extra credit in a course motivated participation. Of the 280 invitees, 258 were Instagram users who provided valid responses. To check the extent of non-respondent bias, we used the comparison method between the two populations. Main characteristics such as age, gender, SNS use, and experience were very similar between the respondents and non-respondents. As such, we concluded that no significant non-response bias was present. All participants used Instagram. The students were enrolled in a program of studies delivered in English. Thus, all were reasonably fluent in English. For the purpose of the study, we focused on Instagram because, among the millennials and Generation Z (aged from 18 to 35), Instagram is the most popular SNS, with a high utilization rate compared with other SNS such as

Facebook. This range of ages also captures a large segment of SNS users (Turel, 2016; Turel and Serenko, 2012). Table III shows the key characteristics of the sample.

	Sample Characteristics (n=258)
Gender	67% female / 33% male
Age (years)	23.5 (18-52), Std Dev. = 5.5
SNS experience (years)	6.1 (0.5-15), Std Dev. = 2.2
SNS usage (minutes per day)	67.3 (0-233), Std Dev. = 46.5
SNS use frequency (per week)	1 day or less: 5.4%
	2-3 days: 2.7%
	3-5 days: 6.2%
	Almost daily: 85.7%

Table III. Sample Characteristics

5. Results

5.1. Preliminary analysis

First, we examined common method bias risk with a marker variable (Lindell and Whitney, 2001). The variable used refers to the level of familiarity/knowledge about the university where this study was conducted. This variable was expected to be unrelated to the key variables used in the study. Results showed 2.9% maximal shared variance with other variables. This value is considered low (Johnson *et al.*, 2011). Thus, the risk of common method bias was deemed to be minimal. Second, the validity and reliability of the measurement instruments were examined. Reliability was acceptable with all constructs present $\alpha \geq 0.9$ [α(peer privacy concern)= 0.94, α(institutional privacy concern)= 0.97, α(SNS addiction)= 0.90, and α(intention to reduce SNS use)= 0.94). Furthermore, a confirmatory factor analysis (CFA) model in AMOS 27 revealed acceptable fit indices (Baumgartner and Homburg, 1996; Doll *et al.*, 1994)($\chi 2$ /df = 2.24, RMSEA = 0.07 (90% CI [0.06, 0.08]), SRMR = 0.06, CFI = 0.92, IFI = 0.92, RFI = 0.84, NFI =0.86, GFI=0.85, AGFI=0.8). The GFI, AGFI, NFI, and RFI were slightly below the 0.9 thresholds, but they exceeded the recommended cut-off value of 0.80 (Baumgartner and Homburg, 1996; Chang and Chen, 2009; Doll *et al.*, 1994; Kim *et al.*, 2004; Lin, 2013, 2008; Liu *et al.*, 2005; Pontiggia and Virili, 2010).

A measurement model was created to verify the reflective constructs' internal consistency, convergent reliability, and discriminatory validity. Table IV demonstrated that all constructs are internally consistent since the composite reliability (CR) results are higher than 0.7. Adequate convergent validity was demonstrated with average variance extracted (AVE) scores above 0.5 (see Table IV). In addition, all loadings were above 0.7, except the items COM2 and SE11, which are very close to 0.7 (see Table V), which suggests a good loading pattern. The items between 0.4 and 0.7 need to be deleted if they affect other measures, such as the AVE and composite reliability, which does not happen in this study (Hair, 2017). Discriminant validity was established with three methods. Firstly, the Fornell-Larcker criterion (Fornell and Larcker, 1981). To support this criterion, the AVE square root of each construct should be higher than the correlation between the constructs, which is verified in this study (see Table IV). The simple exception is the correlation of SNS addiction (ADD) with Compulsion (COM) and with Social-effect (SE). This was expected since SNS addiction is a second-order construct composed of Compulsion (COM) and Social-effect (SE) constructs. Secondly, the loadings should be higher than the cross-loadings (Hair, 2017), which happens in this study (see Table V). Finally, the heterotrait-monotrait ratio (HTMT) should be below 0.9. Based on Table VII, these criteria are met. Thus, we conclude that all constructs have reasonable discriminant and convergent validity. They can therefore be used in the structural model.

Constructs	Mean	SD	CR	PPC	IPC	COM	SE	ADD	RED
Peer privacy concern (PPC)	3.83	1.68	0.953	**0.895**					
Institutional privacy concern (IPC)	4.61	1.66	0.975	0.467	**0.942**				
Compulsion (COM)	2.7	1.41	0.886	0.21	0.095	**0.812**			
Social-effect (SE)	3	1.41	0.878	0.294	0.241	0.731	**0.769**		
SNS addiction (ADD)	2.74	1.26	0.912	0.275	0.188	0.917	0.942	**0.733**	
Intention to reduce SNS use (RED)	3.54	1.83	0.961	0.357	0.275	0.237	0.462	0.387	**0.944**

Table IV. Descriptive statistics, correlations, composite reliability (CR), and average variance extracted (AVE)
Notes: Values in diagonal (bold) are the AVE square root; SD = standard deviation

Constructs	Item	PPC	IPC	COM	SE	RED
Peer privacy concern (PPC)	PPC1	**0.902**	0.368	0.252	0.316	0.316
	PPC2	**0.901**	0.364	0.229	0.267	0.319
	PPC3	**0.931**	0.412	0.172	0.244	0.297
	PPC4	**0.894**	0.5	0.135	0.221	0.35
	PPC5	**0.846**	0.435	0.169	0.279	0.309

Institutional privacy concern (IPC)	IPC1	0.448	**0.943**	0.08	0.226	0.248
	IPC2	0.472	**0.964**	0.1	0.253	0.248
	IPC3	0.444	**0.971**	0.123	0.24	0.262
	IPC4	0.43	**0.957**	0.129	0.24	0.294
	IPC5	0.407	**0.871**	0.129	0.216	0.23
Compulsion (COM)	COM1	0.178	0.09	**0.8**	0.603	0.179
	COM2	0.127	-0.048	**0.668**	0.461	0.071
	COM3	0.201	0.139	**0.843**	0.589	0.209
	COM4	0.17	0.111	**0.873**	0.671	0.293
Social-effect (SE)	SE4	0.274	0.161	0.611	**0.761**	0.325
	SE6	0.178	0.116	0.598	**0.791**	0.356
	SE9	0.284	0.256	0.605	**0.864**	0.491
	SE10	0.181	0.277	0.47	**0.733**	0.323
	SE11	0.209	0.127	0.576	**0.68**	0.268
Intention to reduce SNS use (RED)	RED1	0.355	0.261	0.3	0.518	**0.961**
	RED2	0.282	0.207	0.168	0.353	**0.905**
	RED3	0.364	0.3	0.271	0.449	**0.964**

Table V. Loadings and cross-loadings

Constructs	PPC	IPC	COM	SE	RED
Peer privacy concern (PPC)					
Institutional privacy concern (IPC)	0.489				
Compulsion (COM)	0.237	0.133			
Social-effect (SE)	0.333	0.272	0.874		
Intention to reduce SNS use (RED)	0.376	0.283	0.255	0.513	

Table VI. Heterotrait-Monotrait Ratio (HTMT)

5.2. Structural model

Before assessing the structural model, we used the variance inflation factor (VIF) to test the multicollinearity of all constructs. The VIF values were below 3 (range from 1 to 1.39) (Hair, 2017), which indicates low and reasonable multicollinearity. After establishing validity and reliability, factor scores were extracted, and the model was tested using regression and the PROCESS macro in SPSS 27 (Hayes, 2013). The variable entry order in the hierarchical regression was: [block 1] -- six control variables (gender, age (years), SNS experience (years), SNS usage (minutes per day), SNS use frequency (per week), and SNS addiction); [block 2] -- the main predictors, that is institutional privacy concern and peer privacy concern; and [block 3] -- interaction of institutional privacy concern with peer privacy concern. Table VII shows the results of the hierarchical regression. The results support all three hypotheses. The moderation model explained 26.3% of the variance in intention to reduce SNS use.

	Main Model		
Model Indices Predictors	Base (Controls) Model R^2 = 0.172; R^2 change = 0.172; p<0.001	Main Effect Model R^2 = 0.252; R^2 change = 0.080; p<0.001	Moderation Model (IPCxPPC) R^2 = 0.263; R^2 change = 0.016; p<0.001
Gender (male:1, female: 0)	**-0.155 (0.009)**	**-0.151 (0.008)**	**-0.150 (0.007)**
Age (years)	0.013 (0.823)	0.016 (0.778)	0.027 (0.585)
SNS experience (years)	0.062 (0.297)	0.050 (0.388)	0.055 (0.363)
SNS usage (minutes per day)	**0.116 (0.086)**	0.097 (0.137)	0.093 (0.119)
SNS use frequency (per week)	-0.002 (0.978)	0.017 (0.772)	0.023 (0.689)
SNS addiction	**0.298 (<0.001)**	**0.224 (<0.001)**	**0.221 (0.001)**
Peer privacy concern		**0.219 (<0.001)**	**0.219 (0.001)**
Institutional privacy concern		**0.120 (0.058)**	**0.139 (0.045)**
Institutional privacy concern x Peer privacy concern			**0.120 (0.022)**

Table VII. Path coefficients and model indices
Note: p<0.10 coefficients are bolded

Specifically, peer privacy concern statistically significantly predicted use reduction intentions in both the main effect and moderation models ($\hat{\beta}$=0.219, $p < 0.001$). Thus, H1 was supported - Peer privacy concern increased one's intention to reduce SNS use. Institutional privacy concern was also statistically significant in the main effects model ($\hat{\beta}$=0.120, $p < 0.10$) and the moderation model ($\hat{\beta}$=0.139, $p < 0.05$). Thus, H2 was also supported - Institutional privacy concern increased one's intention to reduce SNS use. The moderator effect of institutional privacy concern on peer privacy concern effect ($\hat{\beta}$=0.120, $p < 0.05$) was also statistically significant. Therefore, H3 is supported - Institutional privacy concern moderates (increased) the effect of peer privacy concern on one's intention to reduce SNS use. This is depicted in Figure 2. It demonstrates that when the level of institutional privacy concern of a user is high, the weight that peer privacy concern receives in one's mental calculus is greater, which ultimately leads to a greater intention to reduce SNS use. Further analysis showed that peer privacy concern influences intention to reduce SNS use only at medium (average) and high (+1 standard deviation above the mean) values of institutional privacy concern. At low levels of institutional privacy concern (-1 standard deviation below the mean), peer privacy concern did not affect the intention to reduce SNS use. This

contingent effect, and the fact that both facets drive corrective behaviors, behooves scholars to focus on both privacy aspects in future studies. Focusing on one aspect can lead to wrong or partial conclusions.

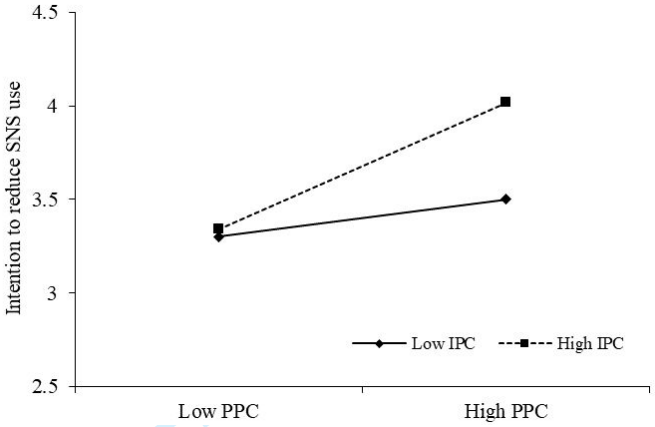

Figure 2. Moderation chart

Regarding the control variables, age, SNS use frequency, SNS experience, and SNS usage were not statistically significant ($p > 0.10$). They did not predict the intention to reduce SNS use. However, SNS addiction increased the intention to reduce use, which is consistent with prior findings on the motivating effect of addiction (Turel, 2015). In addition, gender was significant: males had lower use reduction intentions than females. This may be attributed to more severe body image effects Instagram can have on women, which can increase their use reduction motivation compared to males (Sherlock and Wagstaff, 2019). Such claims, though, merit further research.

6. Discussion

Overall, this study concludes that institutional privacy and peer privacy concern work in tandem to increase one's intention to reduce SNS use. We show direct effects and that institutional privacy concern moderates (strengthens) the relation between peer privacy concern and one's intention to reduce SNS use. Finally, the findings demonstrate that males are significantly less likely than

females to reduce SNS use and that SNS addiction increases one's intention to reduce SNS use. These findings represent essential extensions of the existing literature regarding and scholarly understanding of SNS corrective behaviors, mainly use reduction behavior. An important extension our results provide is the integration of the two facets of privacy concerns (institutional and peer) in one model and hypothesizing and testing their unique and joint effects on use reduction intentions. Considering the unique effects and the "privacy concern transfer" effect, our model explained 26.3% of the variation in intention to reduce SNS use.

The results first directly confirm that the level of concern that users have about the misuse of their personal information by SNS organizations (institutional privacy concern) increases 'users' intentions to reduce SNS use. This conclusion aligns with other studies that found that high levels of institutional privacy concern lead users to avoid SNS use (Zhang et al., 2020), and to become less active, engaged, and prompt to disclose information on SNS (Ayaburi and Treku, 2020; Bansal *et al.*, 2016; Desimpelaere *et al.*, 2020; Dhir *et al.*, 2019; Jozani *et al.*, 2020; Zhou and Li, 2014). This shows that when users are aware of and understand the privacy risks associated with SNS use, they endorse behavioral adjustment (i.e., corrective behaviors) that will help them reduce their privacy risk exposure while still enjoying the benefits of using the SNS. This finding can inform research beyond SNS, for example, works on online banking, interactions with artificial intelligence, and other contexts in which the potency for privacy violation is high, as our findings imply that privacy concerns can motivate behavior changes in the form of use reduction.

Our second finding relates to users' concerns about the potential misuse of personal data entrusted to their peers (peer privacy concern). We show that this concern motivates corrective action by endorsing a reduction in SNS use. This is consistent with prior research findings about the motivating potential of peer privacy concern (Ozdemir *et al.*, 2017). Users aware of and concerned about what their peers might do with the information they share on social media will attempt to reduce SNS use to diminish their risk.

Even though it seems that the effect of peer privacy concern is more significant or in the direction of being more prominent in explaining SNS use reduction, confidence intervals suggest no significant difference. This means that the effects of peer privacy and institutional privacy

concerns are similar. This highlights the importance of focusing on both facets of privacy concerns which at least have identical effects on intentions to reduce SNS use. The literature, thus far, has typically considered only one facet at a time.

Third, we hypothesized and observed a moderating effect. This suggests that the effect of peer privacy concern on use reduction intention is contingent on the level of peer privacy concern. It supports our "privacy concern transfer" argument by showing that concerns about the SNS platform inform the weight of peer privacy concern in one's mental calculus. In line with our expectations, the data showed that institutional privacy concern strengthened the relationship between peer privacy concern and the intention to reduce SNS use.

6.1. Theoretical Implications

Overall, our study makes several significant contributions to the theory. Importantly, it highlights the need to include the two facets of privacy concerns (institutional and peer) in IS studies on corrective behaviors in contexts where peers and institutions can threaten one's privacy. Such contexts are abundant because many modern technologies include social interaction elements. For example, through gamification, websites can encourage social compassion and healthy competitions to promote desirable behaviors such as learning, exercising, information security compliance, and saving money (Klock *et al.*, 2020; Silic and Lowry, 2020; Tu *et al.*, 2019; Zhang *et al.*, 2021). At the same time, such social elements and interactions can drive peer privacy concern, as one exposes their information to others (think about dating websites, social commerce websites, and multiplayer video games). Our findings emphasize the need to consider the threat to users' privacy posed by peers, and not only by the website provider.

Thus, we pave the way for integrating peer and institutional concerns in such models and contexts. We show that scholars need to consider the unique effects of each and their interaction because there is a process of "privacy concern transfer." From a unique effects perspective, we show that, at least in our contexts, peer privacy concern and institutional privacy concern have similar effects on one's mental calculus. There is an opportunity to examine if the balance is equal in another context, or perhaps there are situations where one facet of privacy concerns can be more

influential. We hence call for future studies to consider both facets of privacy simultaneously. Our findings provide the needed theoretical arguments (transfer process) and measures to do so and to extend privacy models from focusing only on the institutional facet, to including peer privacy concern.

Considering the significant interaction, we support the "privacy concern transfer" view and show that privacy concerns about the website inform the weight privacy concerns about peers receive in mental calculus. When the provider is seen as ineffective at catering to one's privacy needs, concerns about peer behavior become more alarming. They are more potent in driving use reduction and perhaps other corrective behaviors. The contingent effect we found here, and the "privacy concern transfer" perspective can be used for extending research in other contexts in which both peers and institutional privacy concerns are at play. For example, one may expect that on dating websites, there is an opportunity for data mistreatment by both peers and the website operator (Lutz and Ranzini, 2017). Thus, future research can examine whether our ideas can help explain why some people change their use patterns of dating websites. It is also essential that future research examines the weight of each privacy facet individually. In this study, we showed that the two facets obtained similar weights in one's mental calculus. However, this may differ in other types of applications (e.g., dating apps), where one factor may have a more considerable weight than the other.

Our findings also allowed us to expand the existing body of knowledge regarding SNS use reduction. With this work, it was possible to evaluate a new perspective on this behavior. Specifically, it was possible to understand the overlooked better by using the two privacy concern facets and assessing their relationship in affecting the SNS use reduction behavior. It understudied SNS corrective behavior of use reduction (Osatuyi and Turel, 2020). This behavior, so far, has received less attention than other types of corrective behaviors (e.g., quitting (Lin *et al.*, 2020; Luqman *et al.*, 2017, 2020; Vaghefi and Qahri-Saremi, 2017)). However, this behavior is essential and can have different drivers and outcomes than more frequently studied behaviors, such as total discontinuance. Our findings thus point to a need to investigate further what motivates the use reduction to correct one's status quo. In line with prior works (Osatuyi and Turel, 2020),we show

that SNS use reduction seems like a reasonable course of action to users. We add to the body of knowledge about the drivers of such behaviors.

Nevertheless, by no means is our model exhaustive. It took just one specific angle to explain this critical behavior. As such, our findings present an opportunity for further studying SNS use reduction and pave the way for understanding the reduction in the use of other IS. Such reduction attempts are dangerous for service providers or internal IT departments, as they may eventually lead to the discontinuance of the use of applications (Furneaux and Wade, 2011). Thus, we call for more research on the drivers of use reduction and for extending our model by considering how the privacy angle can be integrated with other theoretical accounts that might explain use reduction and behavior change.

6.2. Practical Implications

Our study indicates that awareness of the two privacy facets is the key to motivating behavior change (use reduction). Thus, users can be informed by our findings, reflect on the levels of privacy they can live with, and adjust their behavior from an informed standpoint. Because this depends on user awareness of privacy issues, users need to increase privacy literacy. This literacy is insightfully high (Bartsch and Dienlin, 2016). Hence, users can benefit from various training programs that might ensure reasonable levels of privacy literacy (Wissinger, 2017). This privacy literacy can be provided by schools for younger users and by mass media (e.g., television) for all users, especially adults beyond school years. Even governments could intervene by providing the necessary means to allow reaching the most significant number of SNS users. It is crucial that this training touch not only the institutional perspective but also the peer privacy perspective. Users must be aware of all risks they incur when uploading data about themselves.

While it may seem counterproductive, SNS institutions can also provide such training because it might portray them as more caring about users and their need. They may want to mitigate privacy breaches to satisfy their users and guarantee they will continuously use their services. In addition, they need to ensure sufficient privacy protection. As such, the SNS institutions must reduce both

peer and institutional privacy concerns. While we did not explore ways to do so, based on prior research, we can suggest methods such as increasing privacy information transparency and simplicity (e.g., by using privacy labels, warnings, and seals) and using technologies and policies to ensure that privacy violations are minimized (Larose and Rifon, 2007; Lwin *et al.*, 2007; Milne and Culnan, 2004). For example, SNS institutions might consider additional settings allowing users to control better what is shared about them. It is also essential that SNS institutions start involving users in the process of personalizing the privacy settings in a way that guarantees their expectations about privacy protection (Eskens, 2020). With those measures, users may feel safer and have lower privacy concerns.

6.3. Limitations and further research

Despite the contribution of this work, it has significant limitations that point to future research directions. First, this study focused on young adults using a single IS in one country, specifically university students from Portugal that use Instagram. Generalizing to other contexts can be achieved through replication in future research. Second, since this study focused on a privacy angle, possible future studies can extend this view by integrating it with other perspectives on use reduction. Lastly, developing our model and ideas for other dependent variables (behaviors), such as total discontinuance or taking a break from SNS, would be interesting.

7. Conclusion

We revealed here that users decide to reduce their use of SNS through, among other considerations, a mental calculus of their privacy violation risks. These include concerns about peers sharing their information *and* service providers mistreating their information. We show here that both factors are essential and that the effect of peer privacy concern can depend on one's institutional privacy concern. We call for future research to further examine how complex sets of privacy concerns influence information system user behaviors.

Acknowledgments

This research received no specific grant from the public, commercial, or not-for-profit funding agencies.

References

Adjerid, I., Peer, E. and Acquisti, A. (2018), "Beyond the Privacy Paradox: Objective Versus Relative Risk in Privacy Decision Making", *MIS Quarterly*, Vol. 42 No. 2, pp. 465–488.

Ajzen, I. (2012), "The Theory of Planned Behavior", *Handbook of Theories of Social Psychology: Volume 1*, SAGE Publications Ltd, 1 Oliver's Yard, 55 City Road, London EC1Y 1SP United Kingdom, pp. 438–459.

Ayaburi, E.W. and Treku, D.N. (2020), "Effect of penitence on social media trust and privacy concerns: The case of Facebook", *International Journal of Information Management*, Vol. 50, pp. 171–181.

Bansal, G., Zahedi, F.M. and Gefen, D. (2016), "Do context and personality matter? Trust and privacy concerns in disclosing private information online", *Information & Management*, Vol. 53 No. 1, pp. 1–21.

Bartsch, M. and Dienlin, T. (2016), "Control your Facebook: An analysis of online privacy literacy", *Computers in Human Behavior*, Vol. 56, pp. 147–154.

Baumgartner, H. and Homburg, C. (1996), "Applications of structural equation modeling in marketing and consumer research: A review", *International Journal of Research in Marketing*, Vol. 13 No. 2, pp. 139–161.

Bright, L.F., Kleiser, S.B. and Grau, S.L. (2015), "Too much Facebook? An exploratory examination of social media fatigue", *Computers in Human Behavior*, Vol. 44, pp. 148–155.

Cain, J.A. and Imre, I. (2021), "Everybody wants some: Collection and control of personal information, privacy concerns, and social media use", *New Media & Society*, p. 146144482110003.

Chang, H.H. and Chen, S.W. (2009), "Consumer perception of interface quality, security, and loyalty in electronic commerce", *Information & Management*, Vol. 46 No. 7, pp. 411–417.

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., Ping, J.W., Xu, Y. and Tan, B.C.Y. (2015), "Information privacy concern about peer disclosure in online social networks", *IEEE Transactions on Engineering Management*, Vol. 62 No. 3, pp. 311–324.

Cheng, X., Hou, T. and Mou, J. (2021), "Investigating perceived risks and benefits of information privacy disclosure in IT-enabled ride-sharing", *Information & Management*, Vol. 58 No. 6, p. 103450.

Chennamaneni, A. and Taneja, A. (2015), "Communication Privacy Management and Self-Disclosure on Social Media - A Case of Facebook", *AMCIS 2015 Proceedings*, p. 11.

Cho, I.H. (2015), "Facebook discontinuance: discontinuance as a temporal settlement of the constant interplay between disturbance and coping", *Quality & Quantity*, Vol. 49 No. 4, pp. 1531–1548.

Choi, B.C.F. and Land, L. (2016), "The effects of general privacy concerns and transactional privacy concerns on Facebook apps usage", *Information & Management*, Vol. 53 No. 7, pp. 868–877.

Choi, H., Park, J. and Jung, Y. (2018), "The role of privacy fatigue in online privacy behavior", *Computers in Human Behavior*, Vol. 81, pp. 42–51.

Desimpelaere, L., Hudders, L. and Van de Sompel, D. (2020), "Knowledge as a strategy for privacy protection: How a privacy literacy training affects children's online disclosure behavior", *Computers in Human Behavior*, Vol. 110, p. 106382.

Dhir, A., Kaur, P., Chen, S. and Pallesen, S. (2019), "Antecedents and consequences of social media fatigue", *International Journal of Information Management*, Vol. 48, pp. 193–202.

Dinev, T. and Hart, P. (2003), "Privacy Concerns and Internet Use – A Model of Trade-off Factors", *Academy of Management Proceedings*, Vol. 2003 No. 1, pp. D1–D6.

Doll, W.J., Xia, W. and Torkzadeh, G. (1994), "A Confirmatory Factor Analysis of the End-User Computing Satisfaction Instrument", *MIS Quarterly*, Vol. 18 No. 4, p. 453.

Eskens, S. (2020), "The personal information sphere: An integral approach to privacy and related information and communication rights", *Journal of the Association for Information Science and Technology*, Vol. 71 No. 9, pp. 1116–1128.

"Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens". (2018), *The New Work Times*, available at: https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html.

Fornell, C. and Larcker, D.F. (1981), "Evaluating structural equation models with unobservable variables and measurement error", *Journal of Marketing Research*, Vol. 18 No. 1, pp. 39–50.

Fu, S. and Li, H. (2020), "Understanding social media discontinuance from social cognitive perspective: Evidence from Facebook users", *Journal of Information Science*, Vol. 48 No. 4, pp. 544–560.

Furneaux and Wade. (2011), "An Exploration of Organizational Level Information Systems Discontinuance Intentions", *MIS Quarterly*, Vol. 35 No. 3, p. 573.

Gruzd, A. and Hernández-García, Á. (2018), "Privacy Concerns and Self-Disclosure in Private and Public Uses of Social Media", *Cyberpsychology, Behavior, and Social Networking*, Vol. 21 No. 7, pp. 418–428.

Hair, J.F. (Ed.). (2017), *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*, Second edition., Sage, Los Angeles.

Hayes, A.F. (2013), *Introduction to Mediation, Moderation, and Conditional Process Analysis: A Regression-Based Approach*, The Guilford Press, New York.

Hogan, B. (2010), "The Presentation of Self in the Age of Social Media: Distinguishing Performances and Exhibitions Online", *Bulletin of Science, Technology & Society*, SAGE Publications Inc, Vol. 30 No. 6, pp. 377–386.

Hong, W. and Thong, J.Y.L. (2013), "Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies", *MIS Quarterly*, Vol. 37 No. 1, pp. 275–298.

Islam, A.N., Mäntymäki, M., Laato, S. and Turel, O. (2022), "Adverse consequences of emotional support seeking through social network sites in coping with stress from a global pandemic", *International Journal of Information Management*, Elsevier, Vol. 62, p. 102431.

Jiang, Z. (Jack), Heng, C.S. and Choi, B.C.F. (2013), "Research Note —Privacy Concerns and Privacy-Protective Behavior in Synchronous Online Social Interactions", *Information Systems Research*, Vol. 24 No. 3, pp. 579–595.

Johnson, R.E., Rosen, C.C. and Djurdjevic, E. (2011), "Assessing the impact of common method variance on higher order multidimensional constructs.", *Journal of Applied Psychology*, Vol. 96 No. 4, pp. 744–761.

Jozani, M., Ayaburi, E., Ko, M. and Choo, K.-K.R. (2020), "Privacy concerns and benefits of engagement with social media-enabled apps: A privacy calculus perspective", *Computers in Human Behavior*, Vol. 107, p. 106260.

Kehr, F., Kowatsch, T., Wentzel, D. and Fleisch, E. (2015), "Blissfully Ignorant: The Effects of General Privacy Concerns, General Institutional Trust, and Affect in the Privacy Calculus", *Information Systems Journal*, Vol. 25 No. 6, pp. 607–625.

Kim, H.-W., Xu, Y. and Koh, J. (2004), "A Comparison of Online Trust Building Factors between Potential Customers and Repeat Customers", *Journal of the Association for Information Systems*, Vol. 5 No. 10, pp. 392–420.

Kircaburun, K. and Griffiths, M.D. (2018), "Instagram addiction and the Big Five of personality: The mediating role of self-liking", *Journal of Behavioral Addictions*, Vol. 7 No. 1, pp. 158–170.

Klock, A.C.T., Gasparini, I., Pimenta, M.S. and Hamari, J. (2020), "Tailored gamification: A review of literature", *International Journal of Human-Computer Studies*, Vol. 144, p. 102495.

Kuenzler, A. (2022), "On (some aspects of) social privacy in the social media space", *International Data Privacy Law*, Vol. 12 No. 1, pp. 63–73.

Larose, R. and Rifon, N.J. (2007), "Promoting i-Safety: Effects of Privacy Warnings and Privacy Seals on Risk Assessment and Online Privacy Behavior", *Journal of Consumer Affairs*, Vol. 41 No. 1, pp. 127–149.

Liang, K., Liu, J.K., Lu, R. and Wong, D.S. (2015), "Privacy Concerns for Photo Sharing in Online Social Networks", *IEEE Internet Computing*, Vol. 19 No. 2, pp. 58–63.

Lin, H. (2013), "The effects of knowledge management capabilities and partnership attributes on the stage-based e-business diffusion", *Internet Research*, Vol. 23 No. 4, pp. 439–464.

Lin, H.-F. (2008), "Determinants of successful virtual communities: Contributions from system characteristics and social factors", *Information & Management*, Vol. 45 No. 8, pp. 522–527.

Lin, J., Lin, S., Turel, O. and Xu, F. (2020), "The buffering effect of flow experience on the relationship between overload and social media users' discontinuance intentions", *Telematics and Informatics*, Vol. 49, p. 101374.

Lindell, M.K. and Whitney, D.J. (2001), "Accounting for common method variance in cross-sectional research designs.", *Journal of Applied Psychology*, Vol. 86 No. 1, pp. 114–121.

Liu, C., Marchewka, J.T., Lu, J. and Yu, C.-S. (2005), "Beyond concern—a privacy-trust-behavioral intention model of electronic commerce", *Information & Management*, Vol. 42 No. 2, pp. 289–304.

Luqman, A., Cao, X., Ali, A., Masood, A. and Yu, L. (2017), "Empirical investigation of Facebook discontinues usage intentions based on SOR paradigm", *Computers in Human Behavior*, Vol. 70, pp. 544–555.

Luqman, A., Masood, A. and Ali, A. (2018), "An SDT and TPB-based integrated approach to explore the role of autonomous and controlled motivations in 'SNS discontinuance intention'", *Computers in Human Behavior*, Vol. 85, pp. 298–307.

Luqman, A., Masood, A., Weng, Q. (Derek), Ali, A. and Rasheed, M.I. (2020), "Linking Excessive SNS Use, Technological Friction, Strain, and Discontinuance: The Moderating Role of Guilt", *Information Systems Management*, Vol. 37 No. 2, pp. 94–112.

Lutz, C. and Ranzini, G. (2017), "Where Dating Meets Data: Investigating Social and Institutional Privacy Concerns on Tinder", *Social Media*, Vol. 3 No. 1, p. 12.

Lwin, M., Wirtz, J. and Williams, J.D. (2007), "Consumer online privacy concerns and responses: a power–responsibility equilibrium perspective", *Journal of the Academy of Marketing Science*, Vol. 35 No. 4, pp. 572–585.

Maier, C., Laumer, S., Eckhardt, A. and Weitzel, T. (2015), "Giving too much social support: social overload on social networking sites", *European Journal of Information Systems*, Taylor & Francis, Vol. 24 No. 5, pp. 447–464.

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.

Marwick, A. and Ellison, N.B. (2012), "'There Isn't Wifi in Heaven!' Negotiating Visibility on Facebook Memorial Pages", *Journal of Broadcasting & Electronic Media*, Vol. 56 No. 3, pp. 378–400.

Milne, G.R. and Culnan, M.J. (2004), "Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices", *Journal of Interactive Marketing*, Vol. 18 No. 3, pp. 15–29.

Mondal, M., Yilmaz, G.S., Hirsch, N., Khan, M.T., Tang, M., Tran, C., Kanich, C., *et al.* (2019), "Moving Beyond Set-It-And-Forget-It Privacy Settings on Social Media", *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, presented at the CCS '19: 2019 ACM SIGSAC Conference on Computer and Communications Security, ACM, London United Kingdom, pp. 991–1008.

Morlok, T. (2016), "Sharing is (not) caring – the role of external privacy in users' information disclosure behaviors on social network sites", *Pacific Asia Conference on Information Systems (PACIS 2016)*, p. 17.

Niu, G., Yao, L., Tian, Y., Sun, X. and Zhou, Z. (2020), "Information overload and the intention to reduce SNS usage: the mediating roles of negative social comparison and fatigue", *Current Psychology*, pp. 1–8.

Osatuyi, B. and Turel, O. (2020), "Conceptualisation and validation of system use reduction as a self-regulatory IS use behaviour", *European Journal of Information Systems*, Vol. 29 No. 1, pp. 44–64.

Ozdemir, Z.D., Jeff Smith, H. and Benamati, J.H. (2017), "Antecedents and outcomes of information privacy concerns in a peer context: An exploratory study", *European Journal of Information Systems*, Vol. 26 No. 6, pp. 642–660.

Pontiggia, A. and Virili, F. (2010), "Network effects in technology acceptance: Laboratory experimental evidence", *International Journal of Information Management*, Vol. 30 No. 1, pp. 68–77.

Ranzini, G., Newlands, G. and Lutz, C. (2020), "Sharenting, Peer Influence, and Privacy Concerns: A Study on the Instagram-Sharing Behaviors of Parents in the United Kingdom", *Social Media + Society*, Vol. 6 No. 4, p. 205630512097837.

Ravindran, T., Yeow Kuan, A.C. and Hoe Lian, D.G. (2014), "Antecedents and effects of social network fatigue: Antecedents and Effects of Social Network Fatigue", *Journal of the Association for Information Science and Technology*, Vol. 65 No. 11, pp. 2306–2320.

Raynes-Goldie, K. (2010), "Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook", *First Monday*.

Ruths, D. and Pfeffer, J. (2014), "Social media for large studies of behavior", *Science*, Vol. 346 No. 6213, pp. 1063–1064.

Shane-Simpson, C., Manago, A., Gaggi, N. and Gillespie-Lynch, K. (2018), "Why do college students prefer Facebook, Twitter, or Instagram? Site affordances, tensions between privacy and self-expression, and implications for social capital", *Computers in Human Behavior*, Vol. 86, pp. 276–288.

Sherlock, M. and Wagstaff, D.L. (2019), "Exploring the relationship between frequency of Instagram use, exposure to idealized images, and psychological well-being in women.", *Psychology of Popular Media Culture*, Vol. 8 No. 4, pp. 482–490.

Shokouhyar, S., Siadat, S.H. and Razavi, M.K. (2018), "How social influence and personality affect users' social network fatigue and discontinuance behavior", *Aslib Journal of Information Management*, Emerald Publishing Limited, pp. 344–366.

Silic, M. and Lowry, P.B. (2020), "Using Design-Science Based Gamification to Improve Organizational Security Training and Compliance", *Journal of Management Information Systems*, Vol. 37 No. 1, pp. 129–161.

Soliman, W. and Rinta-Kahila, T. (2020), "Toward a refined conceptualization of IS discontinuance: Reflection on the past and a way forward", *Information & Management*, Vol. 57 No. 2, p. 103167.

Tarafdar, M., Maier, C., Laumer, S. and Weitzel, T. (2020), "Explaining the link between technostress and technology addiction for social networking sites: A study of distraction as a coping behavior", *Information Systems Journal*, Vol. 30 No. 1, pp. 96–124.

Taylor, D.G., Davis, D.F. and Jillapalli, R. (2009), "Privacy concern and online personalization: The moderating effects of information control and compensation", *Electronic Commerce Research*, Vol. 9 No. 3, pp. 203–223.

Tu, R., Hsieh, P. and Feng, W. (2019), "Walking for fun or for 'likes'? The impacts of different gamification orientations of fitness apps on consumers' physical activities", *Sport Management Review*, Elsevier, Vol. 22 No. 5, pp. 682–693.

Turel, O. (2014), "Quitting the use of a habituated hedonic information system: a theoretical model and empirical examination of Facebook users", *European Journal of Information Systems*, p. 16.

Turel, O. (2015), "An empirical examination of the 'vicious cycle' of facebook addiction", *Journal of Computer Information Systems*, Vol. 55 No. 3, pp. 83–91.

Turel, O. (2016), "Untangling the complex role of guilt in rational decisions to discontinue the use of a hedonic Information System", *European Journal of Information Systems*, Vol. 25 No. 5, pp. 432–447.

Turel, O. and Qahri-Saremi, H. (2016), "Problematic Use of Social Networking Sites: Antecedents and Consequence from a Dual-System Theory Perspective", *Journal of Management Information Systems*, Vol. 33 No. 4, pp. 1087–1116.

Turel, O. and Serenko, A. (2012), "The benefits and dangers of enjoyment with social networking websites", *European Journal of Information Systems*, Vol. 21 No. 5, pp. 512–528.

Vaghefi, I. and Qahri-Saremi, H. (2017), "From IT Addiction to Discontinued Use: A Cognitive Dissonance Perspective", presented at the Hawaii International Conference on System Sciences, available at:https://doi.org/10.24251/HICSS.2017.681.

Vaghefi, I., Qahri-Saremi, H. and Turel, O. (2020), "Dealing with social networking site addiction: a cognitive-affective model of discontinuance decisions", *Internet Research*, Vol. 30 No. 5, pp. 1427–1453.

Vitak, J. (2012), "The Impact of Context Collapse and Privacy on Social Network Site Disclosures", *Journal of Broadcasting & Electronic Media*, Vol. 56 No. 4, pp. 451–470.

Wang, J., Zheng, B., Liu, H. and Yu, L. (2021), "A two-factor theoretical model of social media discontinuance: role of regret, inertia, and their antecedents", *Information Technology & People*, Vol. 34 No. 1, pp. 1–24.

Wang, Y. and Herrando, C. (2019), "Does privacy assurance on social commerce sites matter to millennials?", *International Journal of Information Management*, Vol. 44, pp. 164–177.

Wissinger, C. (2017), "Privacy Literacy: From Theory to Practice", *Communications in Information Literacy*, Vol. 11 No. 2, pp. 378–389.

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.

York, C. and Turcotte, J. (2015), "Vacationing from Facebook: Adoption, Temporary Discontinuance, and Readoption of an Innovation", *Communication Research Reports*, Vol. 32 No. 1, pp. 54–62.

Yu, L., Li, H., He, W., Wang, F.-K. and Jiao, S. (2020), "A meta-analysis to explore privacy cognition and information disclosure of internet users", *International Journal of Information Management*, Vol. 51, p. 102015.

Zhang, Y., He, W. and Peng, L. (2020), "How Perceived Pressure Affects Users' Social Media Fatigue Behavior: A Case on WeChat", *Journal of Computer Information Systems*, Taylor & Francis, Vol. 62 No. 2, p. Understanding mobile SNS continuance usage in China from the perspectives of social influence and privacy concern.

Zhang, Y., Van Horen, F. and Zeelenberg, M. (2021), "Increasing saving intentions through leaderboards: A gamification approach", *PloS One*, Public Library of Science San Francisco, CA USA, Vol. 16 No. 4, p. e0249283.

Zhou, T. and Li, H. (2014), "Understanding mobile SNS continuance usage in China from the perspectives of social influence and privacy concern", *Computers in Human Behavior*, Vol. 37, pp. 283–289.