
Article:
Muhammad, S.S., Dey, B.L., Bala, H. et al. (2024) A typology and model of privacy- and security-concerned users' attitudes towards digital footprints and consequent influence on their social media adaptation. Journal of the Association for Information Systems, 25 (5). pp. 1240-1273. ISSN: 1558-3457

https://doi.org/10.17705/1jais.00893

A Typology and Model of Privacy- and Security-Concerned Users' Attitudes towards Digital Footprints and Consequent Influence on their Social Media Adaptation

Abstract

How users with privacy and security concerns engage with social media in light of their perceptions of risks associated with their digital footprints is a critical question for research and practice. Using a mixed-methods approach, we examined privacy- and security-related concerns of social media users and their subsequent adaptation behaviors in two studies. The first study, a qualitative enquiry, helped us develop a 2x2 matrix of four groups of social media users with respect to their privacy- and security-related attitudes characterized as careless, carefree, conscious, and cautious. A conceptual model comprised of eight hypotheses was developed based on the qualitative study that captures the relationship between privacy- and security-related attitudes and social media adaptation behaviors. The second study, a quantitative study, tested the model and revealed that users with careless and carefree attitudes were likely to explore social media to maximize benefits and exploit certain applications, while cautious users were likely to avoid using social media. The findings were inconclusive for conscious users' adaptation behaviors, however. This could be due to their systematic and informed decision making, which is likely to have contextual variability. We contribute by offering a clear and coherent typology and model of privacy- and security-concerned users' attitudes and social media adaptation behaviors.

Keywords: social media, digital footprints, privacy, security, adaptation behaviors, attitude

1 Introduction

The innovation and diffusion of digital platforms such as social media (e.g., Facebook and Twitter), business platforms (e.g., Amazon and Alibaba), and service-oriented platforms (e.g., Uber and Airbnb) have significantly transformed our lives (Srivastava & Chandra, 2018; Zifla &

Wattal, 2019). Amongst the various platforms, social media have achieved pervasive reach and popularity by enabling users to create their own content that can be liked and shared by other users (Benbya et al., 2020). Consequently, social media users leave their digital footprints by creating and responding to such content (Müller et al., 2016). Digital footprints embody users' identities, memories, moments, and behaviors, and hold significant value for businesses. Social media providers and other businesses trace and collect digital footprints and establish data connections, inferences, and data interpretations to generate powerful market insights and intelligence (Castillo et al., 2021) that are used by businesses to promote customized products and services (Gunarathne et al., 2018; Sharif & Nazareth, 2021).

Many individuals, however, avoid making their digital footprints public due to privacy and security risks (Gerlach et al., 2019; Lin & Armstrong, 2019). Some users choose to share their personal information and interactions in the form of posts, likes, and comments only with selected individuals and groups (Appel et al., 2020). They may not want these contents displayed and stored on social media, to be accessed and used by other individuals and organizations, because of the fear of undesired consequences including social/occupational embarrassment, financial loss, and threats to their personal wellbeing (Wade et al., 2020). Increasing evidence of privacy and security breaches justifies and reinforces these concerns. For instance, it was reported that a hacker compiled information on 700 million LinkedIn users in pursuit of monetary gains (Tidy, 2021). Also, policy makers worldwide have instituted bans on the use of TikTok on government devices, as the popular platform is alleged to pose national security threats (Cuthbertson, 2023). That said, the number of social media users across the world has increased by 80% since 2017 (Dixon, 2023)[1] despite the concurrent and growing concerns for privacy and security (Han et al., 2021; Provost et al., 2015). The growing need for security calls

upon further research to investigate the ways in which users can negotiate these privacy and security risks while engaging social media.

"Privacy" and "security" have been identified as multi-disciplinary and diverse concepts addressed in a broad range of personal practice and research settings (Awad & Krishnan, 2006; Chanson et al., 2019; Crossler & Posey, 2017; Kartal & Li, 2020). The essence of privacy and security concerns for technology is rooted in a user's perception of risks and uncertainties pertaining to their interaction within digital platforms (Gerlach et al., 2019). While some are indifferent about sharing personal information (Acquisti et al., 2020), others may prefer to take a restrictive and aversive approach (Choi et al., 2015). Different attitudes and perceived levels of risk or security uncertainties would thus determine how they use digital platforms such as social media (Karwatzki et al., 2022). Accordingly, users' varied attitudes toward privacy and security on social media would usher in different types of adaptation behaviors. Therefore, developing a typology of user attitudes toward privacy and security on social media is a crucial first step toward achieving a deeper understanding of how and why different user groups adapt their approaches to platform engagement.

Although prior research has attempted to categorize information systems (IS) users based on their privacy- and security-related attitudes (Elueze & Quan-Haase, 2018; Sheehan, 2002; Wang & Lee, 2020), these classifications are scattered and often fall short of providing a clear, coherent, and nuanced understanding of user social media behavior, either with or without their knowledge of privacy- and security-related risks. Notwithstanding the shortcomings of these typologies, the existing literature has assumed that users' engagement with technologies such as social media are not unidimensional, but involve adaptive behaviors (Schmitz et al., 2016; Turel & Qahri-Saremi, 2023), where exploration and exploitation of a technology are considered as

two major types of adaptive behaviors (Bala & Venkatesh, 2016; Schmitz et al., 2016). Users' assessment of its risks (e.g., privacy and security breach) and benefits will drive their desire to explore or exploit a technology. They may wish to explore various features, but if such exploration involves a higher level of risk, they could adhere to more certain or familiar features and exploit their benefits (Shao et al., 2022). Hence, exploration and exploitation can be deemed as unpredictable behavioral options in light of how users leverage benefits and minimize perceived risks in different ways.

Outside of these two behaviors, however, users not only move along the spectrum between exploration and exploitation, but may also choose to avoid using a technology that they deem harmful or without value (Bala & Venkatesh, 2016; Turel & Qahri-Saremi, 2023). Hence, the inclusion of avoidance can offer a more comprehensive understanding of users' adaptive behaviors. The existing literature, however, has not assessed exploration, exploitation, and avoidance in tandem as possible adaptive social media behaviors in response to users' privacy and security concerns. Accordingly, in the context of such concerns on social media, this research aims to analyze how users with different privacy- and security-related attitudes adapt their social media usage in the form of exploration, exploitation, and avoidance. In so doing, we seek to develop a theory-driven and empirically validated typology of privacy and security attitudes and establish the link between these attitudes and adaptation behaviors.

Using uncertainty reduction theory (URT) as the key theoretical lens, we analyze different types of users' privacy- and security-related attitudes and concerns in the context of social media. URT enables us to categorize people's attitudes and approaches in dealing with uncertain or ambiguous situations, which we apply within the context of users' interaction with social media. To underpin our conceptualization of social media adaptation behaviors, we resort

to adaptive structuration theory (AST), which explains the roles of both the structure of the technology and social interactions of users when engaging the technology (DeSanctis & Poole, 1994). Hence, we integrate two theoretical strands to offer a more holistic understanding of attitude-behavior relationships for social media users concerned with privacy and security.

Employing a mixed-methods approach (Venkatesh et al., 2013; Venkatesh et al., 2016) and following the structure and methodological rigor from exemplars of mixed-methods papers in the IS literature (e.g., Califf et al., 2020), we undertook a layered approach in executing our two studies in which each layer builds on the previous layer. First, we delved into the literature on privacy, security, and adaptation in the context of social media to ascertain the research gaps. Second, we conducted Study 1 to help develop a typology of user attitudes based on a qualitative enquiry and a conceptual model linking these attitudes to social media adaptation behaviors. Third, we tested this model using survey-based quantitative analysis in Study 2.

Our contributions to the literature are threefold. First, the theoretically grounded and robust typology developed in this paper offers a nuanced understanding that privacy and security concerns in the context of social media are not unidimensional. Through our typology of careless, carefree, conscious, and cautious attitudes toward social media risks, positioned within a 2x2 matrix, this paper showcases how users manifest different attitudes toward privacy and security risks on social media platforms. Second, examining the relationship between the different attitudes toward privacy and security and social media adaptation behaviors (e.g., exploration, exploitation, and avoidance) demonstrates the ways in which social media use varies among users. Third, based on the findings, we contribute to the literature by asserting how careless and carefree users are likely to explore and exploit various social media platforms, which leaves their digital footprint, while cautious users tend to avoid them, making their

behavior or specific attitude toward a technology inconclusive.

2 Conceptual Background

2.1 Attitude towards Privacy and Security

Human attitude has been identified as a strong antecedent to behavioral intention that leads to a specific behavioral outcome. Represented as "a summary evaluation of a psychological object captured in such attribute dimensions as good–bad, harmful–beneficial, pleasant–unpleasant, and likeable–dislikeable" (Ajzen, 2001, p. 29), attitude is viewed as an outcome of belief and cognitive processes. Prior research has suggested that both utilitarian and affective considerations influence the use of IS (Bhattacherjee & Sanford, 2006; Jiang et al., 2013). Hence, users' attitude toward privacy and security on social media can be influenced by both cognitive and affective evaluation (Anderson & Agarwal, 2011; Boss et al., 2015).

The reasons behind privacy and security concerns in social media engagement are embedded within users' knowledge and perceptions of the risks and benefits of IS applications. In this paper, we consider privacy and security as a composite concept. Building on prior research, we suggest that in the digital sphere, users' perceptions of privacy are often constituted by their fear of losing resources, threats to personal safety, and negative impacts on career, personal/social status, and psychological state (Karwatzki et al., 2022). As many of these consequences are emblematic of security breaches (Barth et al., 2019; Hsu et al., 2012; Karjalainen et al, 2019), we assert that users' privacy and security concerns for social media engagement ought to be assessed together, as they have significant overlaps and cannot necessarily be disentangled by standard user behavior analysis, or by users themselves (Barth et al., 2019; Bélanger & James, 2020; Karwatzki et al., 2022).

Privacy and security concerns for social media can arise for myriad reasons. The online

world in general and social media in particular have core characteristics such as a lack of compartmentalization and territorialization of identities, which diminish users' control and volition over retaining privacy and security compared to the offline world (Dey et al., 2020). People often do not want to disclose their identity online and may feel uncomfortable with the unknown and/or anonymized users who may have access to their private information (Awad & Krishnan, 2006; Han et al., 2021; Lin & Armstrong, 2019). Higher levels of anonymity on a platform can cause privacy and security concerns that involve individuals' complex perceptual assessments of the actors and processes involved (Jiang et al., 2013). Individuals' confidence subsides and concern for privacy rises when they move from a domain of known people to a borderless territory of strangers, a core characteristic of social media platforms (Teubner & Flath, 2019). Hence, engagement with such platforms has inherent privacy and security risks.

In the context of social media, users can have fear and a sense of threat due to privacy and security risks while simultaneously cherishing a wide range of benefits, such as social support (Huang et al., 2019) and self-expression (Lin & Armstrong, 2019). It is therefore possible that individuals' perceived benefits of using a platform, including social connectivity, information, and entertainment, can outweigh their concerns about privacy and security (Gerlach et al., 2019). This dual perspective of both appreciating social media while fearing its risks can create a privacy and security paradox (Acquisti et al., 2020; Dinev et al., 2015). But as the assessment of the benefits and concerns for privacy is subjective, varying from person to person (Lee & Rha, 2016; Sheehan, 2002), theorizing and examining the relationship between users' privacy and security concerns and their social media adaptation behaviors can offer insights on how to negotiate the privacy and security paradox in social media usage, an increasingly important contemporary issue.

2.2 Existing Typologies of Attitude toward IS Privacy and Security

There have been a few attempts to develop a typology of users and/or attitudes based on individuals' perceptions toward risks, including privacy concerns. Based on how users posit perceived benefits against risks such as privacy, Wang and Lee (2020) identified four user categories for smartphone adaptation: innovators, moderators, conservatives, and laggards. Although this classification offers a useful organizing structure for identifying user types based on their adoption patterns, it does not provide a nuanced perspective on ongoing use and adaptation within the realistic context of user-technology relationship. Specifically, the fact that users may still hold strong privacy expectations from a technology beyond its adoption and initial use is not captured in Wang and Lee's (2020) classification. Elueze and Quan-Haase (2018) suggested a typology of privacy attitudes with five categories: fundamentalists, intense pragmatists, relaxed pragmatists, marginally concerned, and cynical experts. In a similar vein, Sheehan (2002) proposed four categories of internet users: unconcerned, circumspect, wary, and alarmed. Other forms of attitudes, such as privacy cynicism, have also been suggested in prior research (Hoffmann et al., 2016).

The abovementioned typologies have mostly focused on certain demographic denominations rather than on broader attitudinal categories. But user attitudes toward privacy and security on social media is a complicated issue that is not necessarily determined by individual factors such as age and gender (Hey Tow et al., 2010). Teenagers, for instance, although quite keen to engage with social media, are increasingly using strict privacy measures because of their vulnerability in the digital sphere (Kang et al., 2021). Tifferet (2019) found that females on social network sites displayed higher privacy concerns and behaviors than males, but this gender difference correlated to activating privacy settings and untagging photographs,

whereas personal info concerns showed smaller gender differences. Hence, while personal demographics should be considered, privacy and security concerns need to be assessed in terms of users' personal perceptions of risks and uncertainties, which constitute a fundamental reason for user behavior (Kang et al., 2021; Tifferet, 2019). Sheehan's (2002) classification of internet users was based on how users perceived the benefits (e.g., enhanced communications) against the risks (e.g., loss of privacy) is based on interactions in the early stage of their internet adoption, which is now less relevant with the complexities and increased use of social media. Social media use in the current world is much more volitional compared to internet use in the early 21st century, as stricter privacy and security measures are now in place.

2.3 Towards a Theoretically Grounded Typology of Attitude toward Privacy and Security

While the literature on privacy and security concerns on social media is still emerging, the conceptualization of typologies lacks cohesion. This paper delves into uncertainty reduction theory to conceptualize attitudes toward privacy and security and leverage this understanding to build a robust typology. URT (Berger & Calabrese, 1975) enables us to determine why and how users assess risks and uncertainties while engaging with social media. The theory posits that uncertainty makes people skeptical/doubtful and uncomfortable, thus impeding them from making decisions. To ease this discomfort, they will employ different strategies to obtain certainty that renders confidence and develops a positive attitude toward a system or process.

Specifically, by resorting to active and passive uncertainty reduction strategies, users seek conformity with other users as well as structural and regulatory assurance (Srivastava and Chandra, 2018). Users' active information-seeking behavior is considered a precursor to situational normality, whereas their reliance on structural assurance corresponds to a passive attitude toward resolving uncertainty (Jones & Leonard, 2008; Srivastava & Chandra, 2018).

Driven by an active need to reduce uncertainties, users are likely to make informed decisions that make them feel the platform interactions are more secure. If users are not convinced they can reach situational normality, they may remain highly skeptical and alert to risks, and decide not to engage at all. The first category of active behavior, when users tend to assess risks and make calculative measures, exhibits what the literature has categorized as *consciousness* (Thapa et al., 2013; Zollo et al., 2018) in relation to the concern, while the more passive approach has been termed as *cautious* (Hampson et al., 2018; Thapa et al., 2013).

Structural assurance is an important trust-building component and resonates with users' desire for passive uncertainty reduction (Jones & Leonard, 2008; Srivastava & Chandra, 2018). Various attributes of a social media platforms, such as regulations, promises, and procedures, may develop a high level of trust among users, which they may have garnered from their own experience or by observing others. Accordingly, this sense of safety and assurance can propel their unhindered engagement with a social media platform (Hey Tow et al. 2010). Their decision can also be driven by the need to reduce complexities and costs (Kramer, 1999), where users may choose to optimize the benefits of social media engagement while minimizing active information-seeking efforts (Posey et al. 2010).

These assertions make way for the identification of two other possible groups in terms of attitudes toward social media: carefree and carelessness. One group identified as fun-loving or easy going has been termed as *carefree* (Tapp & Clowes, 2002; Rodríguez-Castro et al., 2017). The psychology literature has characterized the carefree state as a lack of worry and anxiety (Verplanken, 2012). This group may be aware of uncertainties and risks, but demonstrates an easygoing approach to addressing them. Another group of individuals who are either unaware of or inattentive to risks and uncertainties (Ram & Chand, 2016) has been termed as having an

attitude of *carelessness,* which can cause counterfactual and unintended behavioral consequences (Teigen, 1998). Careless and carefree attitudes can also be linked with users' habitual proclivity of social media engagement. For example, Dinev et al. (2015) argued that habitual use of social media is linked with individuals' lack of cognitive efforts and/or automatic cognitive heuristics and mental shortcuts. Carelessness also suggests a lack of self-control and planning (Jokela et al., 2014), which can lead to addictive and habitual use of social media (Turel & Serenko, 2012).

Based on these factors, a person's desire/need for situational normality and structural assurance or lack of it can offer a theoretical underpinning to better assess the four types of attitudinal categories (i.e., careless, carefree, conscious, and cautious) in relation to privacy and security concerns addressed in our research. Table 1 provides a brief summary of the four components in light of their theoretical definitions.

Table 1: A Summary of Prior Research Related to Our Typology

Attitudes	Prior Research
Careless	• Rogelberg et al. (2000) in their study of employee attitudes toward surveys identified carelessness as a negligent and inattentive attitude. • Fu et al. (2017) proposed that careless users do not hesitate to follow spammers on microblogs. • Ram and Chand (2016) argued that careless drivers do not pay attention to road security measures and are more likely to cause accidents.
Carefree	• According to Tapp and Clowes (2002), individuals with a carefree attitude are easygoing, uninterested, and casual. • Rodríguez-Castro et al. (2017) identified carefree users as fun-loving and indifferent about risks.
Conscious	• Thapa et al. (2013) argued that conscious travelers normally assess risks and make informed decisions about travel. • Zollo et al. (2018) suggested that socially conscious consumers hold social goals and ideologies, while ethically conscious consumers assess public consequences before making a purchase decision.
Cautious	• While analyzing consumers' propensity to take financial risks, Hampson et al. (2018) found that cautious consumers are frugal and risk-averse. • In an organizational context, cautious individuals exhibit negativity and fear of risks (Palaiou et al. 2016). • Thapa et al. (2013) suggested that cautious individuals are likely to avoid travelling to risky places.

2.4 Adaptation Behavior

Prior literature has focused on several aspects of adaptation, such as adaptation behaviors (Bala

& Venkatesh, 2016), adaptive structuration (DeSanctis & Poole, 1994), coping strategies in user adaptation (Beaudry & Pinsonneault, 2005), and temporal patterns of adaptation (Tyre & Orlikowski, 1994). Structuration theory (Giddens, 1984) provides a powerful theoretical underpinning to study and explain adaptation behaviors. It provides a solid theoretical foundation for addressing technology adaptation at organizational (Tyre & Orlikowski, 1994), group (DeSanctis and Poole, 1994), and individual levels (Dey et al., 2018). DeSanctis and Poole (1994) introduced AST to explain technology adaptation within group decision support systems. Extending structuration theory, AST purports the role of technology in creating/recreating social structures. The knowledge, ability, and interpretation of human agents have reciprocal and iterative relations with technology (Orlikowski, 1992). Human agency is considered as a knowledge-based and voluntarist characteristic, which often involves the desire to create new structures by challenging the rules and practices of an existing structure (Kallinikos et al., 2013). This viewpoint, along with the assertion that a structure can at the same time be an enabler and constraint (Orlikowski, 2000), makes structuration theory relevant to our research context. We explore how social media adaptation stems from the embodiment of the social media structure, which can deter users by posing risks and challenges, while simultaneously offering them a plethora of benefits and encouraging them to continue its usage. A user's intent to follow a specific structure depends upon how they interpret and assess these benefits and challenges. However, as not all users are equally malleable to such structural practices, their adaptive behaviors may create new ways of social media use. Hence, human agents, driven by their attitude toward privacy and security concerns, may either continue to follow an existing structure or choose to create new structures in unpredictable ways.

An increasing number of scholarly works have applied AST to study the use and

adaptation of malleable technology such as mobile computing and social media use (Shao & Li, 2022; Shao et al. 2022). Employing AST to the personal use of technology context, Schmitz et al. (2016) identified two distinct types of adaptive modes based on the exploitative-explorative framework in the organizational learning literature (Benner & Tushman, 2002). Exploitative adaptation involves the use of technology in its usual form with incremental changes so that current needs are better served, considered a more conservative approach. On the other hand, exploratory adaptation involves undertaking divergent structures with potentially dramatic or unanticipated consequences. Therefore, studies of adaptation should take this difference into account by acknowledging the characteristics, challenges, and consequences of both approaches.

Bala and Venkatesh (2016) applied the exploration-exploitation dichotomy in light of benefit-seeking attitudes. That is, users tend to explore and maximize the benefits from a technological application or exploit a certain application for its advantages. They also incorporated avoidance as an additional possible adaptive behavioral outcome, which explains what a user tends to do if they perceive that the risks of using a technology can outweigh the benefits it offers (Bala and Venkatesh, 2016). Again, individuals may not only incrementally or radically change a structure, but could also choose to create a new structure or stick to the old structure by avoiding the technology. Lee et al. (2018) further proposed avoidance as a possible adaptive behavior in light of AST. They argued that avoidance offers an integrative dimension for adaptation, when a technology at hand can be used in different ways or when it is not used at all. By incorporating avoidance as an additional adaptation behavior, a robust conceptual underpinning for adaptation behaviors can be presented.

3 Research Overview: Rationale behind Mixed-methods Design

We undertook a mixed-methods research involving a qualitative and a quantitative study.

Following Venkatesh et al. (2016b), the mixed-methods design for the current study was driven by two research objectives: the qualitative study allowed us to develop a typology of privacy- and security-related attitudes while the quantitative study helped us examine the relationships between privacy- and security-related attitudinal dispositions and social media adaptation behaviors. Due to the scattered and contested conceptual approaches in the existing literature, it is imperative to embark on a qualitative enquiry to ascertain the typology of different attitudes and their probable impacts on social media adaptation behaviors. The qualitative data enabled us to identify the boundary conditions and corroborate them against the existing literature. We used our qualitative data to develop a robust typology and hypothesize their relationships with adaptation behaviors. Subsequently, we conducted a quantitative study through a survey to test the hypotheses and the framework. We adopted a multi-strand design (Venkatesh et al. 2016b), as the interview data were corroborated against the existing literature to develop hypotheses, which were tested through the survey.

Each study on its own would be inadequate to achieve the overarching objectives of this research. The first study does not provide a sufficiently objective and generalizable conclusion, while the second study is based on the first. Hence, the two studies are intertwined and synergistic in achieving the research objectives. Our understanding of meta-inferences, developed through an integration of inferences gained from the qualitative and quantitative components of mixed methods study, utilized the combined methodological undertakings to provide robust theoretical contributions. Our use of meta-inference is underpinned by an overarching abductive approach. As suggested by Venkatesh et al. (2016a), we moved back and forth between the data (both qualitative and quantitative) and relevant theories to theorize the novel findings. Further discussion on meta-inferences is provided later in this paper.

4 Study 1

4.1 Qualitative Study: Design Validity

Following the extant literature (Srivastava & Chandra, 2018; Venkatesh et al., 2013, 2016b), we ensured that our qualitative study involved design, analytical, and inference validity. Design validity denotes the rigor in the design and collection of qualitative data, which is a pre-requisite for the credibility and transferability of findings. Based on Srivastava and Chandra (2018), our design validity was established by selecting appropriate respondents and constructing an interview protocol that could extract insightful and robust responses. To ensure consistency, we developed an interview guide following the past literature and discussion among authors, other academics (with expertise in behavioral studies and IS), and graduate students. This guide, which outlined the purpose of the study and the interview protocols (Saunders et al., 2015), was given to study participants prior to the interviews. We carried out 25 semi-structured interviews based on the interview guidelines of Corbin and Strauss (2014).

A maximum variation sampling method was used to select respondents from various demographic groups with regard to age, gender, income, and occupation. All interviews were conducted in the UK. Appendix A provides a list of respondents and their demographic profiles. Two researchers separately conducted the interviews following a pre-designed interview protocol that reflected the research themes and objectives. Both interviewers shared the interview recordings with the rest of the team after each interview. By the 22nd interview, we found repetition in responses, indicating possible data saturation (Corbin & Strauss, 2014). Accordingly, we stopped the interview process after conducting the 25th interview.

Of the 25 interviewees, 14 were men and 11 were women, with ages ranging from 20 to 58 years. The interviewees' occupational status varied and included students, employed

(academics, accountants, pharmacists, engineers, marketers, bankers, and managers, etc.), and unemployed (e.g., housewives) participants. The participants varied in terms of their use of social media platforms. Each interview lasted around 30 minutes. All interviews were digitally recorded. The recorded interviews were transcribed and analyzed using NVivo 12.

4.2 Qualitative Study: Analysis, Analytical Validity, and Inferences

Analytical validity is required to ensure the credibility, plausibility, and trustworthiness of the data and its contribution to theory development (Venkatesh et al., 2013). We ensured the analytical validity by applying rigor in the collection and analysis of data, as suggested by Srivastava and Chandra (2018). The analysis of data commenced with the creation of a coding template and the identification and classification of themes and constituting codes in light of our research objectives and the existing literature.

We worked with a set of *a priori* codes for adaptation behaviors emanating from the existing literature (Bala & Venkatesh, 2016). Simultaneously, we followed an inductive approach in identifying and classifying codes for users' attitudes toward privacy and security. While screening the interview responses, we kept an open mind in spotting any sections that explicated the participants' perceptions of privacy- and security-related risks, their decision-making processes, their expressed intention to use social media, and the actual nature of this use. Table 2 provides a list of codes.

Coding was independently done by two researchers who meticulously went through the interview transcripts and created codes on NVivo in the first stage. At the second stage, the two researchers reached consensus through discussion and reflection upon existing theories, following the standard and acceptable practice for qualitative data analyses (Bala et al., 2021; Srivastava & Chandra, 2018).

Table 2. List of *a Priori* and Data Driven Codes and Themes

	***A priori* codes**	**First-order codes from data**	**Second-order codes from data**	**Final set of constructs**
Adaptation Behavior	Exploration to maximize benefits, exploitation to maximize benefits, avoidance.	Use of various social media platforms (exploration), benefit-seeking behavior, intent to try new apps (exploration), emotional engagement, risk minimizing behavior, value optimizing behavior (exploitation), preference for particular apps (exploitation), limited use of social media (exploitation), reluctance to use social media (avoidance), very controlled use with high privacy measures.	Trying out different apps to maximize benefits (exploration), limited use to certain level to gain specific benefits (exploitation), limited use of certain apps to gain bare minimum benefits (exploitation), reluctance to use (avoidance), disengaged (avoidance).	Exploration to maximize benefits, exploitation to satisfice benefits, avoidance.
Attitudinal components	No *a priori* codes	Adventurous, lack of knowledge, knowledgeable, indifferent, systematic, and concern for privacy, meticulous, protective, suspicious.	Negligent, careless, easy-going, carefree, systematic and conscious, cautious, alert.	Careless, carefree, cautious, conscious.

Following Califf et al. (2020), we corroborated the codes against the existing literature. The theoretical foundation of the paper evolved over time and was informed by the broader conceptual underpinning of uncertainty reduction and adaptive structuration theories. First-order codes were contrasted against the *a priori* codes identified for adaptation behaviors. Where there were no *a priori* codes (e.g., attitudinal components), we referred back to the literature to find appropriate theoretically defined terminologies that captured the concepts. For instance, driven by URT, we started by identifying codes that explain informed decision making by engaging with various sources of information. URT in our context suggests that users often have the desire to seek further information until they feel the platform is favorable for interaction, which leads to situational normality. To capture this attitude, we derived to two codes at the end of the first round of coding: systematic and meticulous. Subsequently, in the second round of coding we compared the two codes against the literature. We realized that "meticulous" could be captured

by what is described in the literature as “conscious.”

In the final round, by engaging further with the psychology and IS literatures, we asserted that conscious users also engage in systematic decision making. We thus obtained the final construct as “conscious” to mean any response that alludes to systematic decision making in the assessment of risks that could not be classified under any of the existing typologies discussed in the literature review. We found that this conscious attitude captured the notion and was identified as an attitudinal construct in the third (final) order. Accordingly, at the third stage, through rigorous review of the literature and a constant comparison method, we derived seven constructs, including the four attitudinal dispositions and three adaptation behaviors that are grouped separately. Table 3 shows various steps in the coding process that led to four constructs for privacy- and security-related attitudes.

Once the seven constructs had been identified, we conducted axial coding to determine the relationship between user attitudes and adaptation behaviors. As shown in Appendix B2, two researchers conducted this axial coding independently and reached consensus. It was found that certain attitudinal dispositions had positive valence towards certain adaptation behavior(s). For instance, the careless and carefree groups of users were more likely to adapt social media in a positive way to obtain optimum benefits. On the other hand, those with cautious and conscious attitudes were inclined toward aversive behaviors. Hypotheses were drawn based on this analysis and observation.

Table 3. Sample Coding Process [2]

Sample Excerpt	Code by Researcher 1	Code by Researcher 2	Consensus 1st Order Code	2nd Order Code	Final Construct
P5: "I enjoy sharing photos on Instagram. My Insta profile is my virtual self and demonstrates my image online. I enjoy meeting and interacting with new people online." Question: Do you know your followers? P5: "Not most of them. But some of them I have known through online interaction." Question: Are you not worried that your privacy will be in jeopardy? P5: "Not at all. I enjoy exploring the social media world."	Unconcerned	Adventurous	Adventurous	Careless	Careless
"I never came across any incidents that caused theft or personal information leakage due to social media use."	Lack of knowledge	Unaware	Lack of knowledge		
"I am fine with the way things are. I have accounts on Facebook, Instagram, and LinkedIn. I am not a frequent user though. But I like occasional interaction with friends and family and enjoy the connectivity. ... I am not worried about my privacy."	Indifferent	Relaxed	Indifferent	Carefree	Carefree
"Yes; I know that [privacy risk]. But I have to bear with that element of risk. I suppose this is the rule of the game. Nothing is risk-free. I cannot keep everything watertight."	Informed	Knowledgeable	Knowledgeable	Easygoing	
"I am always very particular about my social media use. I use Facebook, WhatsApp and LinkedIn. My Facebook is purely for friends and family. My LinkedIn profile is purely to remain connected with people from relevant professional areas."	Systematic and concern for privacy	Compartmentalized	Systematic	Systematic	Conscious
"It's not just the people who are connected with me on social media; I know many commercial entities can collect information about me. You know about what happened with Cambridge Analytica…. I do not want my 5-year-old's photos to be shared in the public domain."	Meticulous	Application for systematic judgement	Meticulous	Conscious	
"I do not add any colleagues or people whom I do not know on my Facebook. I actually have put my Facebook username in my native language, which is Bengali, so that my work colleagues from other nationalities cannot find me on Facebook."	Protective	Sensitive	Protective	Cautious	Cautious

"My privacy and security are extremely important for me: that is why I am very cautious, and I do not share anything on social media, especially Facebook."	Suspicious	Fearful	Suspicious		

According to Venkatesh et al. (2016b), inference quality depends on two major components: design quality and explanatory quality. The design quality of the qualitative study for this research, as mentioned earlier, was ensured through the selection of an appropriate method (interview), sampling criteria, and the construction of interview protocols. Explanatory quality entails the extent to which credible interpretations were made. In order to maintain the explanatory quality and validity of the qualitative analysis, we followed Sarker and Sarker (2009) by reverting back to the participants and seeking their approval of our analysis and interpretation of their responses.

4.3 Typology of Privacy- and Security-Concerned Users' Attitudes

As discussed in the previous section, the major aim of the qualitative enquiry was to identify and analyze attitudinal components and develop a *prima facie* understanding of their links with adaptation behaviors, which would lead to the development of hypotheses for the second study. We identified and investigated the following four attitudinal components.

Carelessness

Our interview findings identified a particular type of user attitude driven by a lack of attention towards their digital footprints on social media. The attitude is rooted in multiple attributes, including hedonism (e.g., enjoying social interactions) and the desire to take liberties in the process, often underpinned by their confidence in structural assurance. They appear to be interacting with social media with a sense of (relative) safety, and do not generally seek information about associated risks. As one respondent (Participant 5) mentioned:

P5: "I enjoy sharing photos on Instagram. My Insta profile is my virtual self and demonstrates my image online. I enjoy meeting and interacting with new people online."

Question: "Are your profile and posts public?"
P5: "Yes. I have a few hundred followers on Insta."
Question: "Do you know your followers?"
P5: "Not most of them. But some of them I have known through online interaction."
Question: "Are you not worried that your privacy will be in jeopardy?"
P5: "Not at all. I enjoy exploring the social media world."

We note a hint of an adventurous (e.g., carefree) attitude in the above response. The respondent seems rather confident about not having any negative consequences for their social media use, and enjoys follower comments and "likes" while having no interaction with them beyond social media. We also noticed that individuals are often not fully aware of the consequences of privacy issues on social media. They are skeptical about the consequences of compromised privacy and therefore pay little or no attention to any privacy measures, as noted by Participant 16 (P16):

Question: "Have you noticed recently Facebook has offered an option to lock your profile?"
P16: "Yes, I have seen that."
Question: What's your take on that?
P16: "I don't know why people lock their profiles. I receive friend requests from people with locked profiles. If my profile is locked, what is the point of being on social media? It is like I am going to a meeting, but not allowing anyone to see my face or listen to my voice. I have kept my profile for public viewing."
Question: "Do you believe that a lack of privacy measures can get you into trouble?"
P16: "I couldn't care less, to be honest. I don't believe hackers or anyone else will gain from my social media account. All these GDPR[3]-related measures I see these days are extremely bureaucratic. It overcomplicates our lives."

It is evident that some users are not keen on compromising their online freedom, pleasure, and lifestyle by adhering to safety measures. There is also an implicit allusion to trust and confidence in social media platforms, which reduces users' sense of uncertainties. The above opinions are symptomatic of a more careless attitude, based on the social psychology literature (Ward & Meade, 2018). Carelessness denotes an individual's deviance and/or non-compliance towards more systematic decision-making processes, as they resort to short-cut decisional heuristics (Harrison & McLaughlin, 1991). Careless attitudes toward driving regulations can serve as a relevant analogy in this regard. Road accidents are often attributed to drivers' careless attitudes, when drivers do not pay attention to health/wellness factors (e.g., tiredness), safety

measures (e.g., safety belts), and traffic rules (Ram & Chand, 2016). As mentioned by Lawson et al. (2013), carelessness refers to an inattentive, negligent, or heedless attitude, which can extend to personal risk issues in the digital world.

In the IS literature, the careless attitude itself has also been identified as a reason for potential security risks. For instance, Watson (2019) argued that organizational security breaches may happen due to careless employees' inadvertent sharing of personal information and/or failure to comply with security measures (e.g., not logging off the system or not accessing information through public Wi-Fi). It is also argued that careless users are likely to post inappropriate (Robertson & Kee, 2017) and unverified (Chadwick et al., 2018) information on social media. Our findings broadly comply with these assertions. We find that careless social media users demonstrate negligence or ignorance on more than one level. We argue that these careless users are likely to share public posts and photos, and will not hesitate to interact with individuals and organizations beyond their more secure acquaintances. They choose to explore the benefits from social media use even if that means compromising their privacy and security.

Carefree

We found another group of users who acknowledge the importance of online security measures despite being indifferent about applying or following them. In effect, they assume that it is normal to make privacy and security compromises on social media, as Participant 2 mentioned:

P2: "I keep my Facebook profile public. I do not mind people following me. Actually, I try to connect with people for my business purposes and it is helpful to have a public profile.
Question: "Are you not worried that it could leak your personal information and cause troubles?"
P9: "Yes, I know that. But I have to bear with that element of risk. I suppose this is the rule of the game. Nothing is risk-free. I cannot keep everything watertight."

This group of users can be viewed as different from careless users due to their knowledge about risks, which makes them less likely to engage with such risks. As Participant 19 noted:

P19: "I am fine with the way things are. I have accounts on Facebook, Instagram and LinkedIn. I am not a frequent

user though. But I like occasional interaction with friends and family and enjoy the connectivity. …. I am not worried about my privacy."

We term this group "carefree," as similar to the careless group, these users are also driven by structural assurance of social media platform that denotes passive uncertainty reduction strategies. Despite being knowledgeable about the privacy and security issues, they remain relaxed, easygoing, and indifferent to the risks. For instance, a study on sexting showed that people demonstrate a carefree attitude when they assume that the activities involve fewer risks (Rodríguez-Castro et al., 2017). That is, even if carefree users are aware of negative consequences, they are not fearful about them because they may feel the enjoyment/benefits of an act would outweigh the risks and uncertainties. Carefree team supporters within sports, for example, are defined as those who love the entertainment aspect of the game, even if that means that their team loses (Tapp & Clowes, 2002). They are not always driven by the outcome, as long as they enjoy being part of the process or situation. They also stay relaxed and experience less stress over the consequences.

Our findings concur with the above assertion about carefreeness. We find that carefree users are often aware of the consequences of privacy and security breaches. Nevertheless, these risks do not fully deter them from engaging with social media. Yet due to their knowledge of risk, they may choose to have less engagement compared to careless users.

Conscious

On the other side of the spectrum of attitude toward privacy and security on social media, we identified a group of users who follow systematic judgement on dangers associated with their presence in and engagement with social media. They are concerned about their privacy and security, and think carefully about what they post and where, and thus try to avoid any untoward consequences. Respondent 12 mentioned this approach in the following interview:

P12: "I am always very particular about my social media use. I use Facebook, WhatsApp, and LinkedIn. My Facebook is purely for friends and family. My LinkedIn profile is purely to remain connected with people from relevant professional areas. My Facebook account has privacy settings. I do not want to share my personal information and whereabouts with everyone. But my LinkedIn profile is open."

The above excerpt shows that some users have a meticulous approach in selecting social media and are fully aware of the nature and consequences of their interactions. Nevertheless, we sought to obtain a deeper insight into this attitude, as reflected in the following response that extends to concerns for family members:

Question: "How would you describe your engagement with social media?"
P21: "I am extremely careful. To me, social media is a tricky place. I feel like I am in the middle of a big football ground and thousands of people are watching me. It's not just the people who are connected with me on social media; I know many commercial entities can collect information about me. You know about what happened with Cambridge Analytica. I do not want them to have access to my account and personal information. I do not want my five-year-old's photos to be shared in the public domain. I do not want everyone to know where I go, what I eat and with whom I socialize."

The group of users in this "conscious" category demonstrate an active uncertainty reduction strategy. They tend to seek information to make an informed decision on whether or not engaging with a social media platform would be favorable. According to Voss et al. (2013), "consciousness" refers to awareness and attention, suggesting that conscious individuals are driven by both cognitive judgement and affective valence (Zollo et al., 2018). They tend to systematically process, distinguish, and categorize information before they make any decisions on a product or service (Thapa et al., 2013). For social media use, this group of users are likely to make assessments of privacy- and security-related risks. Conscious users thus make thoughtful decisions on whom to follow (Fischer & Reuber, 2011), what to post (Khan, 2017), and how to interact (Chua & Chang, 2016) on social media.

We also find that conscious users make meticulous assessment of benefits against potential risks. Although consciousness reflects users' cognitive attitude, users we interviewed also recognize the affective aspects of social media use. They hope to obtain emotional benefits

by engaging with friends and family, obtaining information, and accessing entertainment. At the same time, they are aware of the risks and control their use by following various policies and procedures. They are keen to minimize the risks while simultaneously seeking ways to make use of social media.

Cautious

We noticed that certain respondents are very cautious about their social media engagement, in being protective, alert, and suspicious, as seen in Respondent 4's comments:

P4: "I do not add any colleagues or people whom I do not know on my Facebook… I use WhatsApp to keep connected with work colleagues, friends, and family members… I actually keep a low profile on social media and make limited use of social media."

Respondent 10 shared a similar sentiment while expressing even more caution:

P10: "My privacy and security are extremely important for me: that is why I am very cautious, and I do not share anything on social media, especially Facebook...Nobody knows much about me on social media: I do not share my date of birth and location on social media. ... I don't want anyone to know about my personal life, what I do, where I live and what I like or dislike."

The above interview excerpts reflect a strong sense of negativity, avoidance, and rejection, exhibiting an extreme form of active uncertainty reduction strategy. We characterized this group as cautious, in line with existing literature that describes cautious individuals as frugal and risk-averse (Hampson et al., 2018), alert and suspicious (Yong et al., 2001), informed and aware (Tseng & Teng, 2016), and resistive (Yngfalk & Yngfalk, 2015). In the social psychology literature, a cautious attitude has been denoted as the opposite of an integrative attitude, as it involves limited intention towards interaction and integration (Demo & Hughes, 1990). For social media use, this group is expected to be extremely sensitive about their privacy and security, and are not hesitant in avoiding social media to minimize risks. Consistent with prior research, we identify cautious users as those who have concerns for privacy and security, and hold an alert, suspicious, and restrictive approach to sharing their digital footprints.

4.4 Typology Summary

Our typology categorizes different user groups who have varied perspectives toward privacy/security concerns and how they choose to engage with such risks in order to optimize their benefits. Based on interview findings, we offer a 2x2 matrix (presented in Table 4) that captures a theoretically grounded typology for privacy and security concerned users. The typology is underpinned by and advances uncertainty reduction theory to explain nuanced classifications of active and passive uncertainty reduction strategies for social media use. The 2x2 matrix is particularly useful in its juxtaposition of users' privacy and security concerns and their intent to engage with risks. In summary, we find that careless users have the least concern for privacy and security. Carefree and conscious groups have knowledge and awareness, but they differ in terms of their attitude toward privacy and security. While conscious users actively seek for information, carefree users tend to rely on structural assurance.

There are further differences between conscious and cautious users proposed in the literature. Thapa et al. (2013) differentiated conscious and cautious attitudes within a travel and tourism context. They found that conscious travelers are willing to travel to risky destinations, but they are conscientious about the risks and may change their travel plans if the risk factors increase (Thapa et al., 2013). In contrast, cautious travelers generally belong to the group who are aversive and unwilling to travel to risky places. Our classification resonates with these characterizations, as we identify conscious social media users as those who choose to be systematic and meticulous in assessing their privacy- and security-related risks. In contrast, cautious users fall at the extreme end of privacy and security concerns, in being suspicious, alert, and risk-aversive.

Table 4. Typology of User Attitudes toward Privacy and Security

	Risk engagement higher (compared to corresponding row)	**Risk engagement lower (compared to corresponding row)**
High privacy and security concern	**Conscious** *(Knowledgeable and aware)* They will take risks with appropriate precautions.	**Cautious** *(Risk averse, alert, and suspicious)* Their engagement with risk is the lowest amongst the four groups. They do not like to take any risks at all.
Low privacy and security concern	**Careless** *(Negligent, inattentive, and heedless)* They may or may not be aware of the risks. However, they are the least likely amongst the four groups to pay attention to any risks.	**Carefree** *(Indifferent and easy-going)* Compared to careless users, carefree users are more risk-averse. However, compared to cautious users, carefree users take more risks because they have low privacy concerns.

The above typology is grounded in URT, wherein conscious and cautious users are found to seek active uncertainty reduction strategies. They would in our context either do a thorough assessment of risks or avoid social media altogether. On the other hand, careless and carefree users often resort to passive uncertainty reduction strategies. Based on their confidence, trust, hedonism, or habit of using social media platforms, they have limited or no hesitation in engaging with risks. Figure 1 demonstrates an indicative positioning of the typology within the quadrants of a graph.

We find that the 2x2 matrix used in this research provides a clear and coherent classification of individuals with varied privacy and security concerns, and their approaches to taking risks in leaving digital footprints during their social media engagement. The typology is robust in defining the essence of privacy and security concerns and articulating the comparative positioning of various users in relation to their propensity to take risks. Grounded in a theoretical base and supported through the qualitative study, the typology therefore confirms the theory that

not all individuals with the same level of privacy and security concerns will engage with social media in the same way.

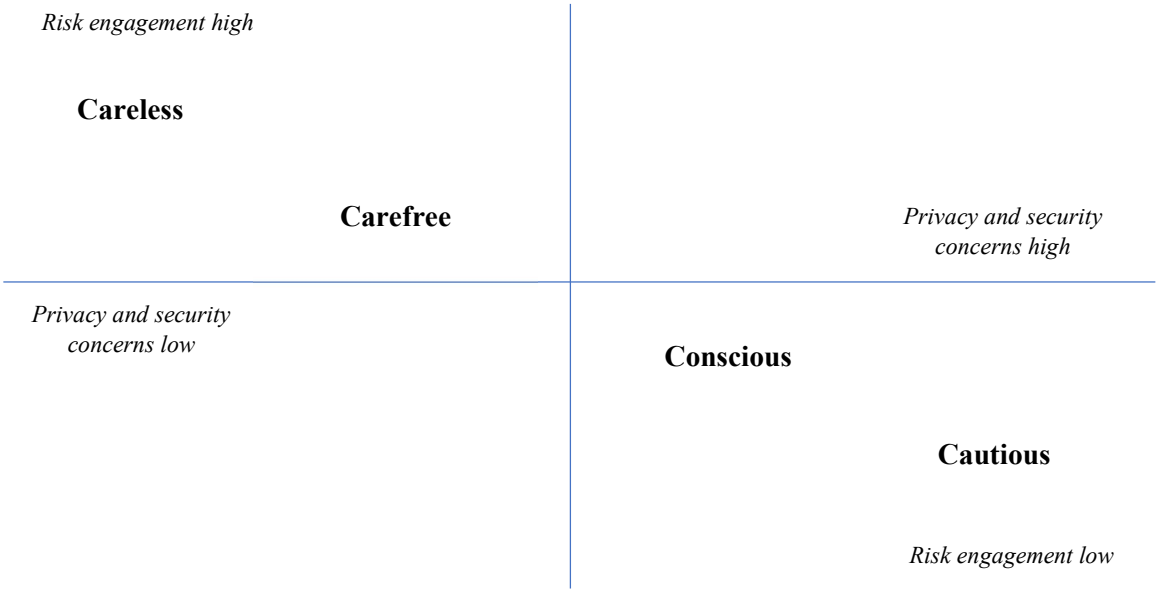

Figure 1: Comparative and Indicative Positioning of the Typology

4.5 Hypotheses Development

The typology developed in Study 1 alludes to plausible ways in which a group of users engage with and adapt social media use. As noted earlier, we moved back and forth between data and literature to ascertain attitudinal components and defined them in relation to specific theoretical and conceptual attributes. We referred back to the extant literature to hypothesize the relationships between our identified attitudes and adaptive behaviors, which were corroborated against the qualitative findings.

Carelessness and Social Media Adaptation

The existing literature also attributes carelessness as an antecedent to non-compliant (Rogelberg et al., 2000) and deviant behavior (Chu & Chau, 2014). Carelessness can also lead to mistakes (Bowling & Huang, 2018; Harrison & McLaughlin, 1991). Fu et al. (2017) argued that individuals with a careless attitude make little or effort to identify risks, nor do they pay attention

to the more systematic processes of cognitive decision making. Hence, their approach to privacy and security management while engaging with social media will be less rigorous. This group may even exhibit a high level of risk-taking proclivity when engaging with social media. Therefore, users with a careless attitude are more likely to fully engage with social media platforms and explore the benefits of social media.

A careless attitude, which can drive impulsive behavior, is also positively correlated with openness to experience and exploration (Dowd & McElroy, 2007), which can lead to innovation and rule breaking. Careless users in the social media context may focus on the opportunities or novelty that a technology provides, regardless of any threats, leading to exploration in obtaining its benefits. For example, Beaudry and Pinsonnault (2005) found that when users perceive a technology as an opportunity (e.g., for entertainment and practice), they are more likely to want to explore it to their advantage. In Study 1, the interview responses concurred with these core characteristics of carelessness and its behavioral outcomes. Interviewee 6 responded:

P6: "I am not worried much about the privacy- and security-related issues. I enjoy trying out new technologies and their applications. I watch movies from streaming services, live sports, use photo editing apps. Some of my friends are skeptical about using these links or apps. I am not. I try to make the optimum use of social media and take everything from it: if that causes me to share my data, I am fine with that."

Hypothesis 1: *Carelessness has a positive effect on social media exploration.*

We hypothesize that users with attitude of carelessness are likely to exploit the benefits of social media. Based on our qualitative data, we further argue that careless consumers are more likely to follow trends without reflecting on any consequences, largely due to their high level of risk engagement combined with low perceived privacy and security concerns. As they do not make efforts to assess the potential risks of digital footprints, they continue to engage with social media in order to receive the bare minimum advantages. Schmitz et al. (2016) applied AST to adaptive behavior analysis involving users' dynamic engagement with structural episodes of a

technology. One of the respondents mentioned during the interview:

P16: "I have multiple social media accounts. I use different social media platforms for different purposes. I use Instagram most. I share photos and experiences. I am not very frequent users of Twitter. But, I use Facebook and LinkedIn quite regularly. I do not use all features of Facebook, I enjoy watching the reels and short clips on Facebook."

Hence, while careless users explore various social media applications, they are also likely to choose particular social media platform and/or application. We argue that careless users would engage with such structural episodes a particular social media application offers, without making a conscious assessment of the privacy- and security-related threats. This group of users are thus likely to employ exploitation or resort to satisficing, where a satisfactory if not optimal choice is made to take advantage of big social media trends, while routinely using common or known features and functionalities of social media.

Hypothesis 2: *Carelessness has a positive effect on social media exploitation.*

Carefreeness and Social Media Adaptation

Tapp and Clowes (2002) described individuals with a carefree attitude as easy-going, uninterested, and casual. They are relaxed, free from care and happy-go-lucky in nature (Chittaro et al., 2017). Because of their general positive outlook on life and specific positive and open attitude towards technology, their perceived benefits of using social media outweigh the risks associated with engaging in social media. We argue that this group of users exhibit an untroubled attitude towards the consequences of their digital footprints and were mainly engaged in social media exploration and exploitation. Those with a carefree attitude are also more open to innovation (Agarwal and Prasad, 1998). Hence, we can argue that that carefree users are likely to take maximum benefits from various social media applications.

The exploration of technological features leads to maximizing innovative ways to use technology and the benefits of these technological features (Thatcher et al., 2010). Carefree

users, despite their lower risk tolerance as compared to the careless group, have knowledge of the benefits of social media, which drives them to engage with the platforms to reap those benefits. Carefree users are indifferent about leaving their digital footprints as they predominantly have trust and confidence in the social media. As a respondent mentioned during the interview:

P8: "I am not too worried about what I share: I share with the people whom I need to share with. I try different apps, although I know some of these apps can be malicious. I cannot afford to subscribe to all these live sports channels. I collect streams from some sports fan groups on Twitter. I know some of these links are dodgy, but it does not concern me. I haven't experienced anything worry so far."

Based on the above conceptual underpinning and interview response, we reach a conjecture that carefree users are likely to undertake exploration of social media.

Hypothesis 3: *Carefreeness has a positive effect on social media exploration.*

Our findings showed that carefree group of users were not concerned about the consequences of their digital footprints and they are likely to explore social media use to maximize benefits. As some of the respondents mentioned:

P9: "I am not much bothered about what I share on social media. Although I am aware of the consequences, I tend not to worry much. I continue to engage with social media. I have 1000 followers and I am not much bothered about what I share on these platforms."

Beaudry and Pinsonnault (2005) suggested that individuals exploit resources to satisfice technological benefits as a routine use of technology, often at the minimal level needed to achieve these features. Technology can be an emergent and enacted structure at the same time, and have embodied and affective properties leading to its continuous use (Orlikowski, 2000). Carefree users who have affective engagement with a technological application are thus likely to make routine and habitual use of the technology. Based on their existing knowledge of social media, and because of their unbothered (Turley, 2005) and indifferent attitude (Chittaro et al., 2017) toward risk, carefree users routinely use the same set of common features of the platform

to perform tasks. That is, they exploit social media benefits via the satisficing decision process, thus making do with suboptimal yet adequate resources (Bala & Venkatesh, 2016).

Hypothesis 4: *Carefreeness has a positive effect on social media exploitation.*

Consciousness and Social Media Adaptation

Conscious users have a relatively lower level of risk-taking and are somewhat more concerned about their privacy and security relative to careless and carefree users. Gibbs et al. (2011) maintained that individuals who are more concerned about their privacy and security tend to achieve situational normality, underpinned by an active uncertainty reduction strategy. Conscious users will actively do their due diligence in terms of researching how to minimize risks of a social media platform or application. They are less likely to have confidence and trust in the process. Accordingly, their engagement with social media would generally be incremental and gradual, as they are reassured by their assessment and judgement of the issue at hand.

Nevertheless, conscious users are least likely to use disruptive adaptive behavior when dealing with unwarranted risks. In the event of higher uncertainties, exploitation of existing resources is generally thought to be more practical than exploration of new opportunities. Hence, an active uncertainty reduction strategy does not engage or encourage exploration. Our qualitative findings are consistent with these arguments. For example, some respondents commented on how privacy concerns on social media posts kept them extra careful, and limit their engagement.

P7: "I am very careful about what I post, which pages I visit and with whom I share my posts. I have privacy measures on Facebook. Because I have a wide range of friends, colleagues, and family members on Facebook, I am extra careful."

P24: "I am very mindful of the fact that we live in a very small globalized village and I don't want what happened to the Prime Minister of Canada with regard to Black Face. I don't want to share on social media [in case] that may happen to me. I think people judge you on social media. Things wouldn't have been like this if we didn't have social media… I do not have Instagram or Snapchat. I only have a Facebook account."

Hypothesis 5: *Consciousness has a positive effect on social media exploitation.*

When conscious users perceive the threats of social media to outweigh its benefits after information-seeking behavior, they may choose to abandon social media altogether. Bala and Venkatesh (2016) argued that when users view a new technology as harmful to their well-being or damaging to their reputation, they are likely to avoid it. Based on the previous literature (Bala & Venkatesh, 2016; Beaudry & Pinsonneault, 2005), we propose that a conscious attitude on the consequences of digital footprints can lead to social media avoidance. These arguments are supported by our Study 1 findings, where Participant 7 noted how Twitter gave too much personal information:

P7: *"I deactivated my Twitter account, since I realized that if someone looks my name up on Google, my tweets pop up. This is not only embarrassing but also can be problematic for my job…. But Facebook is fine, my posts are only for my friends and family."*

Hypothesis 6: *Consciousness has a positive effect on social media avoidance.*

Cautiousness and Social Media Adaptation

The last group of users we investigated has a cautious attitude towards sharing digital footprints on social media platforms, and is very reluctant and skeptical about engaging with social media platforms due to their privacy and security concerns. These users have a distrustful attitude towards the consequences of sharing their digital footprints, which leads them to stay alert, pay attention, and exercise caution toward risk (Fu et al., 2017; Rodríguez-Castro et al., 2017). Karwatzki et al. (2022) found a negative impact of privacy risks on users' willingness to disclose information on a digital platform, despite the benefits of engaging with the digital platform.

Due to their skeptical attitude, some overly cautious users do not think they can achieve situational normality in social media engagement. Even the bare minimum use of social media is not an option in that situation. While we have argued that all other user groups at least engage in exploitation to satisfice social media benefits, we find that this group is reluctant to use it at even

minimum levels. The qualitative findings of interviews corroborate these arguments, as highlighted in the following comment of Participant 13, who even considered not using any technology platforms for communication.

P13: "Sometimes, I feel like I should go back to phone calls or meet face-to-face rather than share anything on these platforms … I would rather have a face-to-face chat or telephone conversation… Social media creates too many unnecessary complexities and risks to justify its use."

Hypothesis 7: *Cautiousness has a negative effect on social media exploitation.*

Prior technology adaptation literature has found that when individuals perceive a technology to bring them harm, they will resort to self-preservation adaptation efforts and reduce the distress caused by the technological disruption. Per the previous interviewee, they may prefer to avoid the technology (Beaudry & Pinsonneault, 2005; Folkman, 1992; Liang & Xue, 2009). Similarly, Bala and Venkatesh (2016) argued that when individuals perceive that a technology is harmful to their well-being, they will explore ways to minimize these harmful consequences, including abandoning the technology.

Cautious users in general exhibit strong skepticism towards using social media platforms, where many avoid them altogether. These users take their privacy concerns seriously and believe that the privacy benefits from abandoning social media platforms outweigh any benefits of using these platforms. Their arguments for privacy are supported by the qualitative findings in Study 1, where one respondent mentioned:

P20: "*I do not share my photos or anything about me on Facebook: again, it is about privacy. I am very careful about what I share on these platforms*."

Hypothesis 8: *Cautiousness has a positive effect on social media avoidance.*

Figure 2 presents the research model based on the hypothesized interrelationships between four types of attitudes and resulting adaptation behaviors.

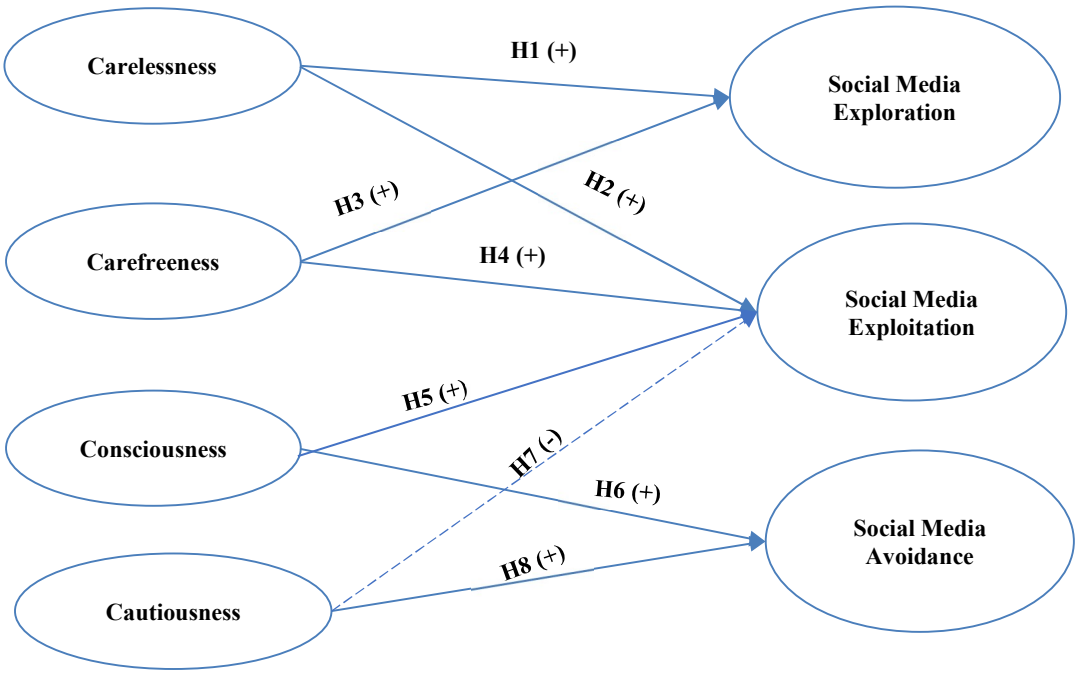

Figure 2: Research Model

5 Study 2

In Study 2, we developed a questionnaire containing seven constructs, derived from Study 1. For content and face validity within the constructs and scales, we followed Churchill's (1979) guidelines. The first step of scale development involved exploring the nature and meaning of each construct in the model and gaining an in-depth understanding of them. This was achieved by means of a literature review and by drawing upon the empirical evidence from Study 1. We adapted existing measurements for all the constructs, and item wordings were also matched with the qualitative findings, as recommended by Churchill (1979), to ensure that the items were abstract and elicited the intended attributes (Rossiter, 2002). Multi-item measures were developed (Table 6) for item specificity and to increase construct reliability.

The findings of the qualitative research reveal users' perspectives on the concepts under investigation. Study 1 also offers insights into conceptualizing and operationalizing the examined variables. The qualitative findings show strong agreement among interviewees that privacy- and security-concerned users in social media exhibit the four attitudes (carelessness, carefreeness, consciousness, and cautiousness) and three adaptation behaviors (exploration, exploitation, and avoidance) that we highlight in our research.

In this study, privacy and security is conceptualized as a composite construct, not least because the prior literature has provided a stronger case for such assertions, particularly in the context of social media (Barth et al., 2019; Hsu et al., 2012; Karjalainen et al, 2019; Karwatzki et al., 2022). In addition to building on prior research, we conducted a separate study with 258 participants to ascertain the validity of our assertion that users perceive privacy and security on social media as a composite (versus unidimensional) concept. Survey questions included three sets of items presented in three question blocks: (a) questions using the word "privacy" only, (b) questions using the word "security" only, and (c) questions using the words "privacy" and "security" together. We presented the question blocks randomly. Our analysis shows that the items from the three sets for the same constructs are highly correlated, and they load together, suggesting that social media users perceive privacy and security concerns in tandem when they think of their digital footprints and risks associated with social media use. In other words, users are not able to separate or disentangle privacy and security concerns and associated risks.

The items for the four attitudinal topologies (i.e., careless, carefree, conscious, and cautious) adapted following prior studies (Hafstrom et al., 1992; Rodriquez-Castro et al., 2017; Thapa et al., 2013; and Yong et al., 2001) are shown in Table 6. The adaptation behavior items were adapted from and Bala and Venkatesh (2016). We validated the scales through a pre-test,

followed by a pilot study conducted on 50 respondents.

5.1 Pre-Test and Pilot Study

For content validation purposes and to identify any inconsistencies before the actual data collection was carried out, we conducted a pre-test (with three academic experts, two practitioners, and 15 social media users) to establish the content validity and face validity. Upon their agreement and satisfaction with the validity of the measures, we then proceeded to test internal consistency via a pilot study. In the pilot study, after questionnaires were administered to a convenience sample of various social media users (e.g., Facebook, LinkedIn, Twitter, Snapchat, Instagram, and WhatsApp), we received 50 useable responses. The results indicated that the four attitude and three adaption behavior constructs had a high level of internal consistency (Cronbach's alpha > 0.70): exploration 0.96, exploitation 0.82, avoidance 0.81, carelessness 0.75, carefreeness 0.77, consciousness 0.81, and cautiousness 0.83. Upon meeting this condition, we proceeded with the data collection for the main study.

5.2 Quantitative Study Results

A final survey of the 733 respondents' profiles revealed that more males than females undertook the survey: around 66% were male and 33% were female. The age spectrum ranged from 18 years to over 65 (Table 5). Around 99% of the respondents were social media users. The main social media platforms used by these respondents were Facebook, Instagram, WhatsApp, YouTube, Twitter, and LinkedIn. The types of digital footprint that users shared on social media were related to shopping, networking, movies/music, information, interests, and likes/dislikes. The highest digital traces shared on these platforms were shopping-related.

Table 5. Sample Characteristics

	Frequency	Percentage of sample
Gender		
Male	488	66%
Female	241	33%
Age		
18-29	298	41%
30-49	383	51.4%
50-64	46	7%
65 years and over	4	0.6%
Social Media		
Users	726	99%
Non-users	7	1%

Data were found to be normally distributed. Skewness and kurtosis fell within the normal range of ±2.0. All constructs were tested for reliability using Cronbach's alpha. Standard deviation, skewness, and kurtosis were measured to check for outliers in assessing the normality of the data following Wilcox's (2011) guidelines. Reliability values of all the constructs were in the acceptable range (> 0.7). Item-to-item correlation values were also in the acceptable range for internal consistency measurement. All constructs had scores above the reference value and thus achieved acceptable internal item consistency.

5.3 Measurement Model Assessment

In order to test the hypotheses, we developed, two types of multivariate analysis were performed: exploratory factor analysis (EFA) and a two-step approach to structural equation modeling (SEM). Explicitly, since the measurements for Study 2 were developed from the established literature, EFA/promax was conducted to identify items that made up Study 2 constructs. The EFA/promax results were then followed up with confirmatory factor analysis (CFA) in the SEM for further tests on reliability and validity. The EFA analysis resulted in a seven-factor solution, with eigenvalues exceeding 1, which accounted for 77.85% of the variance (Appendix C).

We performed a two-step approach to SEM, as suggested by Anderson and Gerbing

(1988). In the first step, a factor analysis was carried out followed by reliability and validity assessment through CFA of the latent constructs for the measurement model. In the second stage, the SEM analysis was undertaken to test for the relationships amongst the latent constructs of the model. The two-step approach tested the measurement model's validity and reliability, and its nomological validity (the full structural model in Step 2), using AMOS version 25 (Arbuckle, 2018). Upon confirmation of validation, nomological validity was tested. The measurement model fitted the data well (Hair et al., 2018): $\chi^2 = 508.349$; $p < .000$; $\chi^2/df = 2.210$; GFI = .942; IFI = .98; TLI = .97; CFI = .98; and RMSEA = .04. Table 6 shows the CFA factor loadings. The construct reliability tests using both composite reliability and Cronbach's alpha all scored above the recommended levels. The correlation among the constructs was also acceptably low, ranging from .02 to .38, and AVE was greater than .50 (Fornell & Larcker, 1981; see Table 7).

Table 6: Scale items, Means, Standard Deviations, Cronbach's Alpha, and Loadings

Constructs	Items	Mean	SD	α	Loading
Social Media Exploration	1. I explore social media to find new ways of sharing information, interests, and memories with others.	3.82	1.15	0.89	0.92
	2. I explore social media for potential new applications to share information, etc.	3.58	1.05		0.81
	3. I experiment with social media to find new features to share information, interests, memories, etc.	3.64	1.14		0.85
Social Media Exploitation	1. I use the same social media features that I learnt from others to share information on social media platforms.	3.61	0.99		0.90
	2. I use common social media features to share my memories, likes, dislikes, and interests etc. with others.	3.59	1.01	0.91	0.92
	3. I use social media features that I learnt from others on these platforms to share my likes, dislikes, interests, information, etc.	3.56	1.10		0.81
Social Media Avoidance	1. I try to avoid sharing information on social media due to my privacy and security.	2.79	1.27	0.93	0.85
	2. I find other ways of sharing information without using social media due to my privacy and security.	2.57	1.19		0.86
	3. I try to perform most of my information sharing without social media due to my privacy and security.	2.91	1.27		0.90
	4. I stay away from sharing my memories, interests, information, etc. on social media as much as I can because of my privacy and security.	2.67	1.22		0.91
Careless	1. I do not care about my privacy and security when I share information on social media.	4.34	0.81	0.91	0.74

	2. I do not take any precautions about my privacy and security when I share information on social media platforms.	4.25	0.82		0.73
	3. I am inattentive to the privacy and security of my digital footprints on social media.	4.17	0.96		0.94
	4. I do not pay attention to my privacy and security when I share information on social media.	4.11	0.99		0.92
Carefree	1. All things considered, there are no privacy and security concerns in sharing information on social media.	2.33	1.12	0.87	0.82
	2. Information sharing is a normal part of social media, due to which I am not worried about my privacy and security.	2.79	1.29		0.80
	3. Information sharing is a regular part of social media, due to which I have no issues with my privacy and security on these platforms.	2.34	1.14		0.87
Conscious	1. I am aware that I will have privacy and security issues if I share information on social media platforms.	2.99	1.29	0.95	0.90
	2. I am aware of the fact that sharing digital footprints on social media has privacy and security risks.	2.92	1.2		0.96
	3. I am aware that sharing digital footprints on social media will have negative outcomes for my privacy and security.	2.91	1.28		0.92
Cautious	1. Sharing information on social media may cause me privacy and security issues in the future.	2.92	1.32	0.95	0.91
	2. Sharing information on social media is a big issue for my privacy and security.	2.98	1.27		0.87
	3. Sharing information, interests, memories, likes and dislikes on social media makes my privacy and security vulnerable.	2.86	1.3		0.95
	4. I am alert about sharing information on social media, as it may cause me privacy and security issues.	2.85	1.29		0.91

A further test to ensure adequate discriminant validity was performed by comparing all the AVE estimates with the square pairwise correlation between factors, and examining cross-loadings among the measured variables and error terms (Hair et al., 2018). Additionally, discriminant validity was confirmed for all latent constructs, since the square root of each construct's AVE was greater than the bivariate correlation (Table 7). At this stage, cross-loadings between both measured and error terms also did not suffer from substantial cross-loadings; standardized residuals were all < 2.58 (Byrne, 2001). Convergent validity was supported, with all parameter estimates > .5 (Kline, 1998). Table 7 shows details of each CFA individual item's convergent validity, and all items were statistically significant at $p < .000$

(Anderson & Gerbing, 1988). Thus, the assessment results support the adequacy of the discriminant validity of our measurement model.

Table 7. Correlation, Reliability and Validity Measures

	1	2	3	4	5	6	7	CR	AVE	MSV	VIF
1. Exploration	**0.86**							0.90	0.74	0.14	1.15
2. Exploitation	0.37	**0.88**						0.91	0.77	0.13	1.17
3. Avoidance	-0.21	-0.16	**0.88**					0.93	0.77	0.21	1.23
4. Careless	0.16	0.09	-0.06	**0.84**				0.90	0.70	0.04	1.03
5. Carefree	0.05	0.12	-0.16	-0.21	**0.83**			0.87	0.70	0.04	1.03
6. Conscious	0.07	0.07	-0.06	0.09	-0.03	**0.93**		0.95	0.86	0.02	1.02
7. Cautious	-0.27	-0.15	0.47	-0.19	-0.16	-0.15	**0.91**	0.95	0.83	0.22	1.12

Note: CR - Composite reliability; AVE – Average Variance Extracted; MSV – Maximum Shared Value; VIF – Variance Inflation Factor
Correlation for all parameters were significant at $p < .000$; Cronbach's alpha coefficients are shown in bold along the diagonal.

5.4 Common Method Variance (CMV) and Endogeneity

Since we used a self-administered survey from a cross-sectional data sample, as an additional check to ensure our model and results were not influenced by common method bias or have an endogeneity issue, we used three different tests: Harman's single factor test (Podsakoff et al., 2003), common latent factor (Collier, 2020), and propensity score matching (PSM) (Rosenbaum and Rubin, 1983).

First, Harman's test was performed, and the result revealed that the total variance explained comes to 24.4% (less than 50%), hence within the recommended limit (Podsakoff et al., 2003). Second, measurement errors were controlled using a single indicator approach where common latent factor is produced, and the scores were then compared with the one without constraints in the hypothesized model (Collier, 2020). The result indicated a lower fit in the constraint model, for example: χ^2 (324) = 13211, $p<.001$); GFI = .384; CFI = .228; TLI: .229; RMSEA = .248; χ^2/df=40.7); hence CMV is not a cause for concern in our study.

Finally, to test for endogeneity, we utilized Rosenbaum and Rubin's (1983) propensity score matching (PSM) using control variables (age, gender, and level of education). We used

carelessness, carefreeness, consciousness, and cautiousness to define the treatment and control groups in this study. We ran PSM in three steps. In the first stage, we used the logit regression. We then split the data into low and high groups for all the attitude variables and estimated the propensity scores that would be used to match individuals through propensity scores. In stage 2, we matched each individual in the treatment group with one individual from the control group with a similar propensity score (1:1 match ratio; Caliper = 0.02; method = nearest matching). We then used a *t*-test to check for differences among gender, age, and level of education, and no significant differences were found. In stage 3, we ran a regression using the attitude variables (carelessness, carefreeness, consciousness, and cautiousness) alongside control variables (age, gender, and education level) on adaptation behaviors (social media exploration, social media exploitation, and social media avoidance).

Our findings are consistent with the results of the baseline (hypothesized) model as follows: careless → social media exploration ($\beta = .64$, $p = .010$); careless → social media exploitation ($\beta = .68$, $p=.008$); carefree → social media exploration ($\beta = .64$, $p = .008$); and carefree → social media exploitation ($\beta = .59$, $p = .007$). Conscious on the other hand was not found to be significant, which is consistent with the main result based on our baseline model, where for example, both social media exploitation ($\beta = .03$, $p = .087$) and conscious → social media avoidance ($\beta = .14$, $p = .056$) indicated insignificant results. Lastly, cautiousness is positively and significantly associated with social media avoidance ($\beta = 1.21$, $p<0.01$). We conclude that endogeneity is not a cause of concern for our study.

5.5 Structural Model Assessment

In Step 2, we assessed the nomological validity of the scales with the three adaptation behaviors and their antecedents. Following the above measurement model procedure, Step 2 was performed

to test all developed hypotheses as well as the nomological validity, and the structural model's results yielded a good fit ($\chi2$= 796, p < .000; $\chi2$/df = 3; GFI = 0.91; IFI = 0.96; TLI = 0.95; CFI = 0.96; RMSEA = 0.05). In total, six hypotheses were accepted with p < .000 and two were rejected. For example, carelessness had a significant positive effect on social media exploration and exploitation, supporting H1 and H2. Similarly, Carefreeness had a significant positive effect on social media exploration and exploitation. Hence, H3 and H4 were supported. However, cautiousness had a negative effect on social media exploitation (p < .020) and a significant positive effect on Social Media Avoidance (p < .000). Therefore, H7 and H8 were also supported. Consciousness did not have a significant effect on social media exploitation (p = .190) and avoidance (p = .809). Hence, H5 and H6 were rejected. Table 8 details the results of all developed hypotheses.

Table 8. Summary of Hypotheses Testing

Hypotheses	β	C.R.	p	Hypothesis
H1 Carelessness → social media exploration	.200	4.459	***	Supported
H2 Carelessness → social media exploitation	.110	2.619	.009	Supported
H3 Carefreeness → social media exploration	.112	2.446	.014	Supported
H4 Carefreeness → social media exploitation	.133	3.101	.002	Supported
H5 Consciousness→ social media exploitation	.040	1.311	.190	Rejected
H6 Consciousness→ social media avoidance	.008	.242	.809	Rejected
H7 Cautiousness → social media exploitation	-.073	-2.323	.020	Supported
H8 Cautiousness → social media avoidance	.436	12.357	***	Supported

Notes: β = Standardized regression weights; CR = Critical Ratio; *** p<0.001.

The effect of carelessness on social media adaptation. We find that careless users are likely to share their digital footprints on social media platforms to explore and exploit their d benefits (as proposed in H1 and H2). A careless attitude makes users inattentive toward and/or ignorant of the potential negative consequences of their digital footprints. This could be due to their lack of attention to risks and harm and/or confidence in the system or structure

(Bhattacherjee et al., 2018; Burns et al., 2017; McKay et al., 2018). As a result, this group of users engage in social media exploration and exploitation.

The effect of carefreeness on social media adaptation. Study results show that carefree users are likely to exhibit social media exploration and exploitation (as hypothesized and supported through H3 and H4). Individuals' positive appraisals are also found to lead to positive adaptive behavior (Bala & Venkatesh, 2016; Wu et al., 2014). As such, individuals who have indifferent perceptions of social media (such as carefree users, per our classification) are likely to explore and exploit social media features (hence, H3 and H4 are supported). As discussed, individuals with a carefree attitude tend to be easy going (Leong et al., 2018). In comparing careless and carefree attitudes, the careless group tends to explore and maximize various social media applications with little or no consideration for the consequences. However, as the carefree group would be more aware of the consequences of sharing their digital footprints on social media, their social media adaptation would be driven by a moderate risk-taking approach.

The effect of consciousness on social media adaptation. As both H5 and H6 were rejected, predictions related conscious users' adaptive behaviors were inconclusive. These users would process information rationally and give considerable attention to a task (Voss et al., 2013), and their privacy/security concerns compel them to choose a systematic and meticulous assessment of risks through extensive information search (Zollo et al. 2018). As this group is driven by informative and systematic decision making, they may choose any of the adaptive behaviors based on prevailing circumstances. Accordingly, we can reach a conjecture that the inter-relationship between their attitude and adaptive behaviors remains inconclusive.

The effect of cautiousness on social media adaptation. Our results show that cautious users are suspiciously alert about sharing their digital footprints on social media platforms, as

they perceive it could harm their well-being. As a result, they do not tend to exploit and instead avoid using social media (both H7 and H8 are supported). A similar notion is echoed in the existing adaptation literature (Bala & Venkatesh 2016), which has posited that individuals would completely abandon a technology when they believe it brings harmful consequences (Bhattacherjee et al., 2018; Liang & Xue, 2009, 2010; Liang et al., 2019). In addition, we find supportive evidence in our qualitative study that users who are extremely cautious towards the consequences of their digital footprints will avoid them altogether.

6 Implications and Conclusions

6.1 Meta-Inference and Theoretical Contributions

Our study confirms that users' attitude toward privacy and security, along with factors influencing their approach/attitude to risk reduction and uncertainties, can influence their social media adaptation behaviors. We advance this understanding by developing a theoretically grounded typology that categorizes users based on four key attitudes toward privacy and security (e.g., careless, carefree, conscious, and cautious).

As discussed, the current typologies of privacy (Elueze & Quan-Haase, 2018; Hoffmann et al., 2016; Sheehan, 2002) do not fully capture social media nuances and are scattered across various literatures. By drilling into exploratory data and corroborating them using the uncertainty reduction theoretical perspective, we create a new typology of attitude toward privacy and security concerns on social media. This approach helps us elucidate how careless and carefree users may have confidence in the structural assurance components of a social media platform. However, a careless attitude could also be a result of a lack of awareness of any risks, and may involve little or no efforts to mitigate them either. On the other hand, many cautious users are highly suspicious of social media, and have little hope for situational normality. These users may

avoid using social media altogether. Conscious attitude in users is generally driven by their pursuit of situational normality, where their adaptation decision would be dependent on the extent to which they can minimize perceived risks. We present this as a clear and coherent typology underpinned by a matrix that contrasts users' engagement with risks in relation to their concerns for privacy and security. Table 9 demonstrates how our categories align with and differ from the existing categories.

Table 9. Typology Comparison

Existing typologies on privacy and security concerns	Relevant construct in our research	Similarities and differences
Fundamentalist users (Elueze & Quan-Haase, 2018) are traditionalist about privacy and fanatical in their desire to keep their private information protected. Alarmed (Sheehan, 2002) users are highly concerned about their privacy online. They are normally educated, and often belong to older age groups.	We define "cautious" users as those who are alert, highly suspicious, and restrictive.	Our term offers a much more inclusive definition and reflects on the underlying cause of this type of attitude. The term "fundamentalist" can be interpreted in multiple ways (often associated with fanaticism). The term "alarmed" captures the meaning of "cautious" but is not as theoretically robust. But cautiousness towards privacy and security is a much clearer lexicon. The term "cautious" captures the notion of risks, which is central to the typological classification.
Pragmatists (Elueze & Quan-Haase, 2018) and Wary internet users (Sheehan, 2002) hold moderate levels of concern regarding privacy.	We define "conscious" users as those who systematically and meticulously process their decisions.	Once again, "conscious" provides a much more inclusive term with a strong theoretical underpinning. Our term alludes to individuals' cognitive decision-making process, a crucial characteristic of consciousness.
Marginally concerned (Elueze & Quan-Haase, 2018) and Circumspect internet users (Sheehan, 2002) have limited concerns about privacy risks.	We define "carefree" as indifference and an easy-going attitude.	"Carefree" offers deeper attitudinal dispositions such as indifference and an easy-going approach. Indifference encapsulates a lack of concern for risks. Also, "carefree" holds inherent affective aspects such as easy-going and fun-loving attitudes, which alludes to stronger attachment to social media use.
Unconcerned users (Sheehan, 2002) have minimal concerns for privacy.	We define "carelessness" as an attitude related to negligence.	The meaning of the word "careless" transcends the "unconcerned" attitude in terms of indifference levels, and it alludes to a clearer and stronger behavioral link.

This research combines uncertainty reduction and adaptive structuration theories to develop a robust understanding of social media users concerned with privacy and security and attitudes that lead to adaptation behaviors. We argue that human agents adapt their behavior to

explore and exploit various aspects of a structure, and may also choose to avoid using it altogether. Their attitude toward a structural episode, along with its features and systems, can determine which adaptation behavior they prefer to undertake. Based on our combined qualitative and quantitative findings, we posit that careless and carefree attitudes will increase the disruptive adaptation (i.e. exploration) of a structural episode. Incremental adaptation (i.e. exploitation), on the other hand, may or may not be driven by consciousness per se. Conscious users' decisions would be determined by their perceived risks-benefits assessment, as a consequence of their information-seeking behavior within a given context. In addition to disruptive and incremental adaptation, we theorize avoidance as a possible adaptive behavior, which may be preferred by the extremely alert group: cautious users.

6.2 Practical and Managerial Implications

This research makes valuable practical and managerial contributions. We suggest that social media providers, practitioners, and policy-makers ought to focus on users concerned with privacy and securities. An enhanced understanding of concerned users' attitudinal attributes and adaptation behaviors, as uncovered in this research, could help guide social media platforms and any future developments designed to increase and maintain a strong user base.

Specifically, social media platforms can segment and profile users based on attitudinal factors, and develop effective targeting strategies using the framework developed in this study. Social media developers can also benefit from this typology, in that they can provide greater flexibility that benefits wider groups of customers. For instance, Facebook's provision to customize the privacy of a post can offer assurance to conscious customers in particular. Snapchat and Facebook Story provide temporary time-bound posts that can reduce the risks of perpetual digital footprints. Carefree and careless users can also benefit from the proliferation of

apps and their desire to have a presence in the digital world. LinkedIn, for example, serves as a near-official résumé in the digital world.

Social media platforms can optimize social media value propositions for privacy- and security-concerned users using the framework to build strong relationships with them. Simultaneously, organizations can reduce social media churn by catering to the needs of conscious and cautious users. Third-party organizations intending to promote products on social media would also benefit from considering these attitudinal dispositions we investigate, and using them to make a calculated approach toward specific groups. However, cautious and conscious users are less likely to welcome unsolicited marketing campaigns. Consent for cookies, as practiced in many European countries due to GDPR, is a sensible approach that is increasingly common in many organizations worldwide.

Despite the gains that social media has enjoyed in recent years, issues such as misinformation and social media data manipulation by the likes of Cambridge Analytica have triggered huge resentment in various quarters. Our research shows that such abusive developments in information gathering are counterproductive, and government intervention is welcomed to ensure healthy and sustainable use of social media and its many positive contributions.

6.3 Limitations and Future Research

This research makes valuable contributions and offers insightful findings by articulating a typology for users concerned with privacy and security in social media. Whilst the findings advance our current understanding of technology adaptation and users' attitudes towards privacy and security on social media, the study has limitations. First, to examine user attitudes and adaptation behaviors toward the consequences of their digital footprints, this research was

carried out with social media users. It does not focus on any particular type of social media, however, and users' perceptions of and engagement with various social media platforms would vary. Moreover, the privacy and security measures on various social media platforms are not the same. Hence, a study on a specific social media platform could provide deeper insights and offer further practical and theoretical implications. Future research could look at users' attitudes and adaptation behaviors in popular social media platforms (e.g., Facebook or Instagram). Particular focus on demographic denominations and customer churn can also offer fresh insights on the nuances of use, adaptation, and avoidance of social media.

Second, technology use (Ferratt et al., 2018; Muhammad et al. 2022) and adaptation (Dey et al., 2018) involve dynamic processes. As users' levels of understanding and expertise evolve with their continuous use of the same technology over a period of time, they may remain conscious (e.g., careful) at the early stage of technology use and gradually change their attitude in light of gained experience and expertise. Our research does not capture this dynamic and evolving nature of users' attitudes. Hence, this paper cannot ascertain whether or not individuals would retain the same attitude over the years, and how their attitudes can change due to differing circumstances. Future research could undertake a longitudinal study to assess whether or not users' attitudes change with evolutions in time and other circumstances. It also remains to be seen whether a conscious user maintains the same attitude/approach across all of the various social media platforms or at all use levels, and whether it will change.

7 Conclusion

Privacy and security concerns surrounding social media use are quite topical in the current environment of rapidly advancing technology. Our research addresses this issue by providing robust theoretical contributions and insightful practical implications. We offer a novel typology

to capture users' attitudes and the influence of these attitudes on their adaptive behaviors, which advances our current understanding of information security and technology adaptation. These findings allude to paradoxes and idiosyncrasies pertaining to user coping strategies for managing privacy and security concerns. Our model can be used to segment social media users based on attitude and behavior patterns, and to design and develop appropriate security measures. The implications of these developments transcend the social media context and provide important guidelines for users, designers, and managers of technology and platforms.

References

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2020). Secrets and likes: The drive for privacy and the difficulty of achieving it in the digital age. *Journal of Consumer Psychology*, 30(4), 736-758.

Agarwal, R., and Prasad, J. 1998. "A Conceptual and Operational Definition of Personal Innovativeness in the Domain of Information Technology," Information Systems Research, 9(2), pp. 204-215.

Ajzen, I. (2001). Nature and operation of attitudes. *Annual Review of Psychology*, 52(1), 27-58.

Anderson, J. C., & Gerbing, D. W. (1988). Structural equation modeling in practice: A review and recommended two-step approach. *Psychological bulletin*, 103(3), 411.

Anderson, C. L., & Agarwal, R. (2011). The digitization of healthcare: Boundary risks, emotion, and consumer willingness to disclose personal health information. *Information Systems Research*, 22(3), 469-490.

Arbuckle, J. L. (2018). Amos (Version 25.0) [Computer Program]. Chicago: IBM SPSS

Appel, G., Grewal, L., Hadi, R., & Stephen, A. T. (2020). The future of social media in marketing. *Journal of the Academy of Marketing Science*, 48(1), 79-95.

Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly*, 13-28.

Bala, H., Hossain, M.M., Bhagwatwar, A. and Feng, X. (2021). Ownership and governance, scope, and empowerment: How does context affect enterprise systems implementation in organisations in the Arab World? *European Journal of Information Systems*, 30(4), 425-451.

Bala, H., & Venkatesh, V. (2016). Adaptation to information technology: A holistic nomological network from implementation to job outcomes. *Management Science*, 62(1), 156-179.

Barth, S., de Jong, M. D., Junger, M., Hartel, P. H., & Roppelt, J. C. (2019). Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematics and informatics*, 41, 55-69.

Bhattacherjee, A., & Sanford, C. (2006). Influence processes for information technology acceptance: An elaboration likelihood model. *MIS Quarterly*, 805-825.

Bhattacherjee, A., Davis, C. J., Connolly, A. J., & Hikmet, N. (2018). User response to mandatory IT use: A coping theory perspective. *European Journal of Information Systems*, 27(4), 395-414.

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

Benner, M. J., & Tushman, M. (2002). Process management and technological innovation: A longitudinal study of the photography and paint industries. *Administrative Science Quarterly*, 47(4), 676-707.

Beaudry, A., & Pinsonneault, A. (2005). Understanding user responses to information technology: A coping model of user adaptation. *MIS Quarterly*, 29(3), 493-524.

Benbya, H., Nan, N., Tanriverdi, H., & Yoo, Y. (2020). Complexity and information systems research in the emerging digital world. *MIS Quarterly*, 44(1), 1-17.

Berger, C., & Calabrese, R. (1975). Some explorations in initial interaction and beyond: Toward a developmental theory of interpersonal communication. *Human Communication Research*, 1(2), 99-112.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*, 39(4), 837-864.

Bowling, N. A., & Huang, J. L. (2018). Your attention please! Toward a better understanding of research participant carelessness. *Applied Psychology*, 67(2), 227-230.

Burns, A.J., Posey, C., Roberts, T.L. & Lowry, P.B. (2017). Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. *Computers in Human Behavior,* 68, 190-219.

Byrne, B. M. (2001). *Structural equation modeling with AMOS: Basic concepts, applications, and programming*. New Jersey, NJ: Lawrence Erlbaum Associates.

Califf, C. B., Sarker, S., & Sarker, S. (2020). The Bright and Dark Sides of Technostress: A Mixed-Methods Study Involving Healthcare IT. *MIS Quarterly*, 44(2), 809-856.

Castillo, A., Benitez, J., Llorens, J., & Braojos, J. (2021). Impact of social media on the firm's knowledge exploration and knowledge exploitation: The role of business analytics talent. *Journal of the Association for Information Systems*, 22(5), 1472-1508.

Corbin, J., & Strauss, A. (2014). *Basics of qualitative research: Techniques and procedures for developing grounded theory*. Los Angeles, CA: Sage.

Chadwick, A., Vaccari, C., & O'Loughlin, B. (2018). Do tabloids poison the well of social media? Explaining democratically dysfunctional news sharing. *New Media & Society*, 20(11), 4255-4274.

Chanson, M., Bogner, A., Bilgeri, D., Fleisch, E., & Wortmann, F. (2019). Blockchain for the IoT: privacy-preserving protection of sensor data. *Journal of the Association for Information Systems*, 20(9), 1274-1309.

Chittaro, L., Sioni, R., Crescentini, C., & Fabbro, F. (2017). Mortality salience in virtual reality experiences and its effects on users' attitudes towards risk. *International Journal of Human-Computer Studies*, 101, 10-22.

Choi, B. C., Jiang, Z., Xiao, B., & Kim, S. S. (2015). Embarrassing exposures in online social networks: An integrated perspective of privacy invasion and relationship bonding.

Information Systems Research, 26(4), 675-694.
Chu, A. M., & Chau, P. Y. (2014). Development and validation of instruments of information security deviant behavior. *Decision Support System*s, 66, 93-101.
Chua, T. H. H., & Chang, L. (2016). Follow me and like my beautiful selfies: Singapore teenage girls' engagement in self-presentation and peer comparison on social media. *Computers in Human Behavior*, 55, 190-197.
Churchill Jr, G. A. (1979). A paradigm for developing better measures of marketing constructs. *Journal of Marketing Research*, 16(1), 64-73.
Collier, J. E. (2020). *Applied structural equation modeling using AMOS: Basic to advanced techniques*. Milton Park, UK: Routledge.
Crossler, R., & Posey, C. (2017). Robbing Peter to pay Paul: Surrendering privacy for security's sake in an identity ecosystem. *Journal of the Association for Information Systems*, 18(7), 487-515.
Cuthbertson, A. (2023) ' TikTok ban in numbers: charting the controversial rise of the world's most popular app', *The Independent*, Tuesday 21 March. Available at: https://www.independent.co.uk/tech/tiktok-ban-map-charts-latest-b2305131.html (Accessed: 08/04/2023).
DeSanctis, G. and Poole, M.S. (1994), Capturing the complexity in advanced technology use: Adaptive structuration theory, *Organization Science*, 5(2), pp. 121-147.
Demo, D. H., & Hughes, M. (1990). Socialization and racial identity among Black Americans. *Social Psychology Quarterly*, 364-374.
Dey, B.L., Balmer, J.M.T., Pandit, A., & Saren, M. (2018). Selfie appropriation by young British South Asian adults: Reifying, endorsing and reinforcing dual cultural identity in social media. *Information Technology and People*, 31(2), pp. 482-506.
Dey, B. L., Yen, D., & Samuel, L. (2020). Digital consumer culture and digital acculturation. *International Journal of Information Management*, 51, 102057.
Dinev, T., McConnell, A. R., & Smith, H. J. (2015). Research commentary—informing privacy research through information systems, psychology, and behavioral economics: Thinking outside the "APCO" box. *Information Systems Research*, 26(4), 639-655.
Dixon, S. (2023) ' Number of social media users worldwide from 2017 to 2027, *The Independent*, 13 February. Available at: https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/ (Accessed: 12/05/2023).
Dowd, K., & McElroy, T. (2007). Susceptibility to anchoring effects: How openness-to experience influences responses to anchoring cues. *Journal of Judgment and Decision Making,* 2(1), 48-53.
Elueze, I., & Quan-Haase, A. (2018). Privacy attitudes and concerns in the digital lives of older adults: Westin's privacy attitude typology revisited. *American Behavioral Scientist,* 62(10), 1372-1391.
Ferratt, T.W., Prasad, J. & Dunne, E.J. (2018). Fast and slow processes underlying theories of information technology use. *Journal of the Association for Information Systems,* 19(1), 1-22.
Fischer, E., & Reuber, A. R. (2011). Social interaction via new social media: (How) can interactions on Twitter affect effectual thinking and behavior? *Journal of Business Venturing*, 26(1), 1-18.

Folkman, S. (1992). Making the case for coping. In B. N. Carpenter (Ed.), *Personal coping: Theory, research, and application*, Westport, CT: Praeger.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error: Algebra and statistics. *Journal of Marketing Research,* 18(3), 382-388.

Fu, H., Xie, X., Rui, Y., Gong, N. Z., Sun, G., & Chen, E. (2017). Robust spammer detection in microblogs: Leveraging user carefulness. *ACM Transactions on Intelligent Systems and Technology (TIST)*, 8(6), 83.

Gerlach, J., Buxmann, P. & Dinev, T. (2019). "They're all the same!" Stereotypical thinking and systematic errors in users' privacy-related judgments about online services. *Journal of the Association for Information Systems,* 20(6), 787-823.

Gibbs, J. L., Ellison, N. B., & Lai, C. H. (2011). First comes love, then comes Google: An investigation of uncertainty reduction strategies and self-disclosure in online dating. *Communication Research*, *38*(1), 70-100.

Giddens, A. (1984). *The Constitution of Society: Introduction of the Theory of Structuration*, Berkeley, CA: University of California Press.

Gunarathne, P., Rui, H., & Seidmann, A. (2018). When social media delivers customer service: Differential customer treatment in the airline industry. *MIS Quarterly*, 42(2), 489-520.

Hair, J., Anderson, R., & Babin, B. (2018). *Multivariate data analysis* (8th edition). Hampshire, UK: Cengage Learning.

Hafstrom, J. L., Chae, J. S., & Chung, Y. S. (1992). Consumer decision-making styles: comparison between United States and Korean young consumers. *Journal of consumer Affairs*, *26*(1), 146-158.

Hampson, D. P., Grimes, A., Banister, E., & McGoldrick, P. J. (2018). A typology of consumers based on money attitudes after major recession. *Journal of Business research*, 91, 159-168.

Han, X., Wang, L., & Fan, W. (2021). Is hidden safe? Location protection against machine-learning prediction attacks in social networks. *MIS Quarterly*, 45(2), 821-858.

Harrison, D. A., & McLaughlin, M. E. (1991). Exploring the cognitive processes underlying responses to self-report instruments: effects of item context on work attitude measures. *Academy of Management Proceedings,* 1991(1), 310-314).

Hey Tow, W. N. F., Dell, P., & Venable, J. (2010). Understanding information disclosure behaviour in Australian Facebook users. *Journal of Information Technology*, 25(2), 126-136.

Hoffmann, C., Lutz, C., & Ranzini, G. (2016). Privacy cynicism: A new approach to the privacy paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 10(4), 7.

Hsu, C., Lee, J. N., & Straub, D. W. (2012). Institutional influences on information systems security innovations. *Information Systems Research*, *23*(3-part-2), 918-939.

Huang, K. Y., Chengalur-Smith, I., & Pinsonneault, A. (2019). Sharing is caring: Social support provision and companionship activities in healthcare virtual support communities. *MIS Quarterly*, 43(2), 395-424.

Jiang, Z., Heng, C. S., & Choi, B. C. (2013). Research note—privacy concerns and privacy-protective behavior in synchronous online social interactions. *Information Systems Research*, 24(3), 579-595.

Jokela, M., Elovainio, M., Nyberg, S. T., Tabák, A. G., Hintsa, T., Batty, G. D., & Kivimäki, M.

(2014). Personality and risk of diabetes in adults: Pooled analysis of 5 cohort studies. *Health Psychology*, 33(12), 1618.
Jones, K., & Leonard, L. N. (2008). Trust in consumer-to-consumer electronic commerce. *Information & Management*, 45(2), 88-95.
Kallinikos, J., Aaltonen, A., & Marton, A. (2013). The ambivalent ontology of digital artifacts. *MIS Quarterly,* 37(2), 357-370
Kang, H., Shin, W. & Huang, J. (2021). Teens' privacy management on video-sharing social media: the roles of perceived privacy risk and parental mediation. *Internet Research*, 32(1), 312-334.
Kartal, H. B., & Li, X. B. (2020). Protecting privacy when sharing and releasing data with multiple records per person. *Journal of the Association for Information Systems*, 21(6), 1465-1485.
Karjalainen, M., Sarker, S., & Siponen, M. (2019). Toward a theory of information systems security behaviors of organizational employees: A dialectical process perspective. *Information Systems Research*, *30*(2), 687-704.
Karwatzki, S., Trenz, M., & Veit, D. (2022). The multidimensional nature of privacy risks: Conceptualisation, measurement and implications for digital services. *Information Systems Journal*, *32*(6), 1126-1157.
Khan, M. L. (2017). Social media engagement: What motivates user participation and consumption on YouTube? *Computers in Human Behavior*, 66, 236-247.
Kline, R. B. (1998). *Principles and practice of structural equation modeling*. New York, NY: The Guilford Press.
Kramer, M. W. (1999). Motivation to reduce uncertainty: A reconceptualization of uncertainty reduction theory. *Management communication quarterly*, 13(2), 305-316.
Lawson, A. R., Pakrashi, V., Ghosh, B., & Szeto, W. Y. (2013). Perception of safety of cyclists in Dublin City. *Accident Analysis & Prevention*, 50, 499-511.
Lee, J. Y. H., Panteli, N., Bülow, A. M., & Hsu, C. (2018). Email adaptation for conflict handling: A case study of cross-border inter-organisational partnership in East Asia. *Information Systems Journal*, *28*(2), 318-339.
Lee, S. M., & Rha, J. S. (2016). Personalization privacy paradox and consumer conflict with the use of location-based mobile commerce, *Computers in Human Behavior,* 63, 453-462.
Leong, L. Y., Jaafar, N. I., & Ainin, S. (2018). The effects of Facebook browsing and usage intensity on impulse purchase in f-commerce. *Computers in Human Behavior*, 78, 160-173.
Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly*, 71-90.
Liang, H. & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*. 11(7), 394-413.
Liang, H., Xue, Y., Pinsonneault, A., & Wu, Y. A. (2019). What users do besides problem-focused coping when facing IT security threats: An emotion-focused coping perspective. *MIS Quarterly*, 43(2), 373-394.
Lin, S., & Armstrong, D. (2019). Beyond information: The role of territory in privacy management behavior on social networking sites. *Journal of the Association for Information*

Systems, 20(4), 434-475.
McKay, A. S., Garcia, D. M., Clapper, J. P., and Shultz, K. S. (2018). The attentive and the careless: Examining the relationship between benevolent and malevolent personality traits with careless responding in online surveys. *Computers in Human Behavior*, 84, 295-303.
Muhammad, S. S., Dey, B. L., Alwi, S. F. S., Kamal, M. M., & Asaad, Y. (2022). Consumers' willingness to share digital footprints on social media: the role of affective trust. *Information Technology & People*, 36(2), 595-625.
Müller, O., Junglas, I., Brocke, J.V. & Debortoli, S. (2016). Utilizing big data analytics for information systems research: Challenges, promises and guidelines. *European Journal of Information Systems*, 25(4), 289-302.
Orlikowski, W. J. (2000). Using technology and constituting structures: A practice lens for studying technology in organizations. *Organization Science,* 11(4), 404-428.
Orlikowski, W. J. (1992). The duality of technology: Rethinking the concept of technology in organizations. *Organization Science*, 3(3), 398-427.
Palaiou, K., Zarola, A., & Furnham, A. (2016). The dark side of personality predicts positive and negative work attitudes. *Personality and Individual Differences*, 88, 12-16.
Podsakoff, N. P., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, 88(5), 879-903.
Posey, C., Lowry, P. B., Roberts, T. L., & Ellis, T. S. (2010). Proposing the online community self-disclosure model: The case of working professionals in France and the UK who use online communities. *European Journal of Information Systems*, 19(2), 181-195.
Provost, F., Martens, D., & Murray, A. (2015). Finding similar mobile consumers with a privacy-friendly geosocial design. *Information Systems Research*, 26(2), 243-265.
Ram, T., & Chand, K. (2016). Effect of drivers' risk perception and perception of driving tasks on road safety attitude. *Transportation Research Part F: Traffic Psychology and Behaviour*, 42, 162-176.
Robertson, B. W., & Kee, K. F. (2017). Social media at work: The roles of job satisfaction, employment status, and Facebook use with co-workers. *Computers in Human Behavior*, 70, 191-196.
Rodríguez-Castro, Y., Alonso-Ruido, P., González-Fernández, A., Lameiras-Fernández, M., & Carrera-Fernández, M. V. (2017). Spanish adolescents' attitudes towards sexting: Validation of a scale. *Computers in Human Behavior*, 73, 375-384.
Rogelberg, S. G., Luong, A., Sederburg, M. E., & Cristol, D. S. (2000). Employee attitude surveys: Examining the attitudes of noncompliant employees. *Journal of Applied Psychology*, 85(2), 284-293.
Rosenbaum, P. R., & Rubin, D. B. (1983). The central role of the propensity score in observational studies for causal effects. *Biometrika*, 70(1), 41-55.
Rossiter, J. R. (2002). The C-OAR-SE procedure for scale development in marketing. *International Journal of Research in Marketing*, 19(4), 305-335.
Sarker, S., & Sarker, S. (2009). Exploring agility in distributed information systems development teams: An interpretive study in an offshoring context. *Information Systems Research*, 20(3), 440-461.

Saunders, M., Lewis, P., & Thornhill, T. (2015). *Research methods for business students*. Harlow, UK: Pearson.

Schmitz, K. W., Teng, J. T., & Webb, K. J. (2016). Capturing the complexity of malleable IT use. *MIS Quarterly*, 40(3), 663-686

Shao, Z., Li, X., & Wang, Q. (2022). From ambidextrous learning to digital creativity: An integrative theoretical framework. *Information Systems Journal*, 32(3), 544-572.

Shao, Z., & Li, X. (2022). The influences of three task characteristics on innovative use of malleable it: An extension of adaptive structuration theory for individuals. *Information & Management*, 59(3), 103597

Sharif Vaghefi, M., & Nazareth, D. L. (2021). Mining online social networks: Deriving user preferences through node embedding. *Journal of the Association for Information Systems*, 22(6), 1625-1658.

Sheehan, K. B. (2002). Toward a typology of Internet users and online privacy concerns. *The Information Society*, 18(1), 21-32.

Srivastava, S.C., & Chandra, S. (2018). Social presence in virtual world collaboration: An uncertainty reduction perspective using a mixed methods approach. *MIS Quarterly,* 42(3). 779-803.

Tapp, A., & Clowes, J. (2002). From "carefree casuals" to "professional wanderers": Segmentation possibilities for football supporters. *European Journal of Marketing*, 36(11-12), 1248-1269.

Teigen, K. H. (1998). Hazards mean luck: Counterfactual thinking in reports of dangerous situations and careless behavior. *Scandinavian Journal of Psychology*, 39(4), 235-248.

Teubner, T., & Flath, C. M. (2019). Privacy in the sharing economy. *Journal of the Association for Information Systems*, 20(3), 213-242.

Tidy, J. (2021). How your personal data is being scraped from social media. *BBC.* Retrieved from: https://www.bbc.co.uk/news/business-57841239.

Tifferet, S. (2019). Gender differences in privacy tendencies on social network sites: A meta-analysis. *Computers in Human Behavior*, 93, 1-12.

Thapa, B., Cahyanto, I., Holland, S. M., & Absher, J. D. (2013). Wildfires and tourist behaviors in Florida. *Tourism Management*, 36, 284-292.

Thatcher, J. B., McKnight, D. H., Baker, E. W., Arsal, R. E., & Roberts, N. H. (2010). The role of trust in postadoption IT exploration: An empirical examination of knowledge management systems. *IEEE Transactions on Engineering Management*, 58(1), 56-70.

Tseng, F. C., & Teng, C. I. (2016). Carefulness matters: Consumer responses to short message service advertising. *International Journal of Electronic Commerce*, 20(4), 525-550.

Turel, O. & Qahri-Saremi, H. (2023). Responses to ambivalence toward social networking sites: A typological perspective. *Information Systems Journal*, 33(2), 385-416.

Turel, O., & Serenko, A. (2012). The benefits and dangers of enjoyment with social networking websites. *European Journal of Information Systems*, 21, 512-528.

Turley, D. (2005). Death, where is thy sting? Mortality and consumer motivation in the writings of Zygmunt Bauman. In S. Ratneshwar, & D.G. Mick (Eds.), *Inside Consumption.* Abingdon, UK: Routledge, 89-107.

Tyre, M. J., & Orlikowski, W. J. (1994). Windows of opportunity: Temporal patterns of

technological adaptation in organizations. *Organization Science*, 5(1), 98-118.
Venkatesh, V., Bala, H. & Sambamurthy, V. (2016a). Implementation of information and communication technology in a developing country: A multimethod longitudinal study in a bank in India. *Information Systems Research,* 27(3), 558-579.
Venkatesh, V., Brown, S. A. & Sullivan, Y. W. (2016b). Guidelines for conducting mixed-methods research: An extension and illustration. *Journal of the Association for Information Systems,* 17(7), 435-495.
Venkatesh, V., Brown, S. A., & Bala, H. (2013). Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. *MIS Quarterly*, 37(1), 21-54.
Verplanken, B. (2012). When bittersweet turns sour: Adverse effects of nostalgia on habitual worriers. *European Journal of Social Psychology*, 42(3), 285-289.
Voss, U., Schermelleh-Engel, K., Windt, J., Frenzel, C., & Hobson, A. (2013). Measuring consciousness in dreams: The lucidity and consciousness in dreams scale. *Consciousness and Cognition*, *22*(1), 8-21.
Wade, J. T., Roth, P. L., Thatcher, J. B., & Dinger, M. (2020). Social media and selection: Political issue similarity, liking, and the moderating effect of social media platform. *MIS Quarterly*, 44(3), 1301-1357.
Wang, X., & Lee, K. M. (2020). The paradox of technology innovativeness and risk perceptions–A profile of Asian smartphone users. *Telematics and Informatics*, 51, 101415.
Ward, M. K., & Meade, A. W. (2018). Applying social psychology to prevent careless responding during online surveys. *Applied Psychology*, 67(2), 231-263.
Watson, H. J. (2019). Update tutorial: Big Data analytics: Concepts, technology, and applications. *Communications of the Association for Information Systems*, 44(1), 21.
Wilcox, R. R. (2011). *Introduction to robust estimation and hypothesis testing.* Oxford, UK: Academic Press.
Wu, Y., Choi, B., Guo, X. & Chang, K.T. (2014). Understanding user adaptation toward a new IT system in organizations: A social network perspective. *Journal of the Association for Information Systems.* 18(11), 787-813.
Yngfalk, C., & Yngfalk, A. F. (2015). Creating the cautious consumer: Marketing managerialism and bio-power in health consumption. *Journal of Macromarketing*, 35(4), 435-447.
Yong, H. H., Gibson, S. J., de L. Horne, D. J., & Helme, R. D. (2001). Development of a pain attitudes questionnaire to assess stoicism and cautiousness for possible age differences. *The Journals of Gerontology Series B: Psychological Sciences and Social Sciences*, 56(5), P279-P284.
Zifla, E. & Wattal, S. (2019) Understanding IT-enabled social features in online peer-to-peer businesses for cultural goods. *Journal of the Association for Information Systems*, 20(5), 629-646.
Zollo, L., Yoon, S., Rialti, R., & Ciappei, C. (2018). Ethical consumption and consumers' decision making: The role of moral intuition. *Management Decision*, 56(3), 692-710.

[1] Number of worldwide social network users 2027 | Statista

[2] Further sample coding is provided in Appendix B1 and B2.

[3] GDPR: General Data Protection Regulation law, enacted by the European Union in 2018.