Dispositional Mindfulness as an Antecedent of Privacy Concerns: A Protection Motivation Theory Perspective[1]

Athina Ioannou
School of Hospitality and Tourism Management
University of Surrey, United Kingdom
Email: a.ioannou@surrey.ac.uk

Iis Tussyadiah
School of Hospitality and Tourism Management
University of Surrey, United Kingdom
Email: i.tussyadiah@surrey.ac.uk

Alaa Marshan
Department of Computer Science
Brunel University, London, UK
Email: alaa.marshan@brunel.ac.uk

Accepted for publication in
Psychology & Marketing
2nd June 2021

Acknowledgements
This work was part of the PRIvacy-aware personal data management and Value Enhancement for Leisure Travellers (PriVELT) Project, funded by the UK's Engineering and Physical Sciences Research Council (EPSRC) under grant number EP/R033196/1.

[1] Citation: Ioannou, A., Tussyadiah, I., Marshan, A. (2021). Dispositional mindfulness as an antecedent of privacy concerns: A protection motivation theory perspective. Psychology & Marketing.

Abstract

This study investigates the effects of mindfulness, an important personality trait, on people's perceptions of privacy. Using protection motivation theory as a conceptual foundation, the central tenet is that mindfulness plays an important role in people's threat appraisal process of privacy concerns and thus influences one's intention to share personal information online. A survey-based approach was employed to measure privacy attitudes of 685 UK individuals about online data disclosure. Our findings demonstrate that mindfulness contributes to the formation of privacy concerns. A more mindful consumer is more likely to adopt a more objective appraisal style, interpret privacy threats as less threatening, and thus share personal information online.

Keywords: mindfulness, privacy concerns, disclosure, online, individual differences

1. Introduction

The public are growing more concerned about online privacy. Almost 79% of people surveyed in the United States (US) reported that they are worried about the amount of personal information collected by companies (Auxier & Rainie, 2019) while 40% of people report that they feel no control over their personal data. During the last decade more than seven billion identities have been exposed in data breaches (Alohali, Clarke, Li, & Furnell, 2018) while numerous privacy breaches in large companies come to light every day, such as the hacking of 57 million Uber user accounts, which included names, addresses, and driver license numbers of Uber drivers (Bradely, 2019). These events can result in users limiting the use of products or services that involve extensive sharing of personal data, bringing important implications for data-driven companies.

However, not all people behave in the same way during privacy decision making. For example, concerned about their privacy, some people might decide to share less information with online providers, while others might refuse to share any information at all. Human decision making is very complex (Mirsch, Lehrer, & Jung, 2017) and privacy behaviour has been described as rather surprisingly diverse. A prominent example can be found in the 'privacy paradox' phenomenon, where individuals express their concerns about their privacy, however they don't act accordingly to protect their personal details online (Kokolakis, 2017). As consequences of privacy concerns, such as limitation or refusal of data sharing, prove to be detrimental for companies and organisations that collect users' personal information, it is imperative to understand in more depth why consumers behave differently during privacy decision making including how they evaluate privacy concerns and threats. Ultimately, this understanding will inform the development of tools or methods to accommodate consumers' privacy preferences, ease privacy concerns and help them make decisions that are in their best interests.

While most studies that have investigated privacy have focused on examining the consequences of privacy concerns on behavioural outcomes such as information disclosure, a growing body of research has focused on exploring the aspects that affect the formation of privacy concerns. Previous research has argued that individual factors, more specifically personality traits, can significantly influence one's perceptions of privacy (Junglas, Johnson, & Spitzmüller, 2008). That is, concerns about privacy can be explained to some degree by personality characteristics. Personality traits can be defined as one's "dispositions or tendencies that lead to certain attitudinal and behavioural patterns in certain situations" (Junglas et al.,

2008, p. 391). As such, individual differences may result in differential reactions during privacy decision making. Indeed, Egelman and Peer, (2015b) demonstrated that individual differences are predictors of differences in privacy attitudes. The majority of systems and online platforms have been designed based on the myth of 'the average user'; however, no one fits in this category perfectly (Egelman & Peer, 2015a). For example, the default privacy settings in a social networking site such as Facebook will not accommodate all users due to varying privacy preferences. As differences in privacy preferences can be attributed to individual differences (Egelman & Peer, 2015a), the investigation of the role of personality traits in decision making can contribute to a deeper understanding of privacy decision making, explaining whether a certain effect is stronger for individuals who show a higher or lower level in personality traits.

Research in information systems (IS) has started to examine the impact of individual differences on privacy and security attitudes (Egelman & Peer, 2015b). While the impact of big five personality traits on privacy attitudes has been the focus of most investigations, other personality traits have been largely disregarded in this context (Egelman & Peer, 2015b). Recently, the concept of mindfulness as a personality trait has attracted increasing attention. A wealth of evidence has demonstrated the beneficial effect that mindfulness has on psychological and physical health such as improvements in individual well-being, reduced levels of stress and anxiety (Tomlinson, Yousaf, Vittersø, & Jones, 2018). Mindfulness is also associated with enhanced professional outcomes such as increased job satisfaction and performance due to the ability to counteract the negative effects of information overload and technostress, detect phishing attacks (Ioannou & Papazafeiropoulou, 2017; Jensen, Dinger, Wright, & Thatcher, 2017). Mindfulness plays a significant role in fostering a lower threat appraisal of stressful events, such as daily stress or demanding life events, facilitating "…non-defensive processing of threatening experiences" (Weinstein, Brown and Ryan, 2009, p. 376). Mindfulness can thus be influential in individuals' privacy threat appraisals (Wirth, Laumer, Maier, & Weitzel, 2017). Moreover, mindfulness is considered a malleable trait that can be cultivated through various interventions such as training programs. Therefore, understanding how mindfulness can influence the formation of individual privacy concerns can bring important implications both at individual consumer level as well as organisational level.

Following existing work on individual differences and threat appraisal of privacy concerns (Junglas et al., 2008), in this study, we aim to explore the impact of dispositional (trait) mindfulness on individual privacy concerns. To achieve this aim, this study adopts protection motivation theory (PMT) (Rogers, 1975), which explains how individuals appraise threats and reveals how personality traits impact the appraisal of those threats. As individual

concerns over privacy can be interpreted as threats, PMT is considered the appropriate theoretical lens for this empirical examination (Junglas et al., 2008). This study seeks to advance current understanding on the influence of trait mindfulness on privacy attitudes and offers important practical implications pertaining to the integration of individual factors in the design and development of technological solutions and digital tools by providers in order to help consumers in privacy decision making.

2. Theoretical Background

The following sections will present the underlying theoretical framework of the current study. This study adopts Protection Motivation Theory (PMT), focusing on the effect of dispositional mindfulness on individual privacy concerns and information disclosure intention as a privacy-related outcome. Grounded on PMT, mindfulness is considered the personality trait that is the source of intrapersonal information triggering an individual's cognitive mediating process, while privacy concerns are considered a threat during this process, resulting in protection motivation and risk reducing behaviours. In this study context, this protection motivation refers to the prevention of privacy losses caused by information collection, use, and sharing practices of online providers.

2.1 Individual Differences and Privacy Concerns

The recent and significant innovations in information technologies accompanied by the extensive adoption of the Internet, personal devices (e.g., smartphones, tablets, and laptops), social networking sites (SNS), and emerging technological solutions (e.g., artificial intelligence, Internet of things, wearable devices, sensors) have made the topic of information privacy more current than ever (Baruh, Secinti, & Cemalcilar, 2017). Privacy is understood as a multifaceted concept encompassing various dimensions (e.g., physical privacy, information privacy) and perspectives (e.g., legal, technical) (Dinev & Hart, 2004; Heravi, Mubarak, & Raymond Choo, 2018). Particularly, online privacy is defined as one's ability to control the uses of their personal information in digital environments, including those related to the collection and dissemination of the information by other entities and organisations (Heravi et al., 2018; Pavlou, 2011).

Being used as proxy to measure privacy, privacy concerns refer to one's "beliefs about the risks and potential negative consequences associated with sharing information" (Baruh et al., 2017, p. 27), including risks such as privacy breaches and privacy invasion, and are

associated with the inherent concern about the possibility of losing personal information while utilising various online environments (P. Li, Cho, & Goh, 2019). Previous research has identified and categorised the antecedents of privacy concerns investigated by previous studies, presented them in groups of factors as: individual characteristics (e.g., personality traits, demographics, psychological factors), macro-environmental factors (e.g., culture, government regulations), information contingencies (e.g., information sensitivity), and social factors (e.g., social norms). Prior research has mostly concentrated on the examination of the outcomes of privacy concerns rather than their antecedents (Smith, Dinev, & Xu, 2011).

Scholars have attempted to better comprehend the influence of individual factors on decision making process related to privacy. Investigating the role of the Big Five personality traits on privacy, Yeh *et al.* (2018) found that only one of the traits, agreeableness, showed an influence on privacy concerns in an electronic commerce context. Inconsistent findings regarding the effects of agreeableness on privacy concerns were noted. Junglas, Johnson and Spitzmüller (2008) found that individuals who are highly agreeable, thus trust others more, are less suspicious of their environment, are less likely to appraise privacy threats as harmful, showing lower privacy concerns than less agreeable people (Junglas, Johnson and Spitzmüller, 2008). However, Osatuyi (2015) found that people who are characterised with higher agreeableness and conscientiousness are more concerned over their privacy in social media platforms.

Other studies have investigated the effects of other individual differences on privacy attitude, demonstrating that individual differences relating to risk taking and decision making are stronger predictors when compared to the Big Five personality traits (Egelman & Peer, 2015b). Moreover, recently Aivazpour and Rao (2019) examined the role of impulsivity and the urge to act spotaneously without thinking about the future consequences of one's actions, on information disclosure aiming to explain the privacy paradox. Results suggest that only one component of impulsivity (i.e., motor impulsivity) affects online data sharing, encouraging increased sharing of personal information. Yao, Rice and Wallis (2007) showed that the need and desire for privacy in the physical world (i.e., privacy disposition) and self-efficacy are the main determinants of online privacy concerns. They concluded that privacy disposition positively influences one's thresholds and tolerance to privacy threats in online environments, while self-efficacy reduces the level of anxiety associated with one's concerns over privacy. Dinev and Hart (2006) found that strong interest in social issues and knowledge in governmental policies and initiatives translates in placing greater importance in privacy, thus increasing one's concerns over online privacy. Recent research has investigated the impact of

privacy awareness, defined as the accumulated knowledge of an individual through the media and other resources (e.g., campaigns, tutorials) as well as previous (negative) experiences related to privacy (e.g., privacy invasion or breach). Benamati, Ozdemir and Smith (2017) demonstrated that people who have higher awareness of privacy related issues, both from the media and previous experiences, reported more concerns about their information privacy.

While scholars have investigated how individual factors explain and predict privacy attitudes and behaviour, additional research is imperative to identify the influence of other personality traits such as mindfulness. The significance of mindfulness is evident during the last few years where scientific research shows an exponential growth of trajectory, reaching more than 30,000 publications in 2015 (MAPPG, 2015; Van Dam et al., 2018). Literature has provided evidence on the wealth of benefits that mindfulness offers by improving psychological well-being and enhancing physical health, bringing important implications for individuals both in their personal as well as professional lives (Davis & Hayes, 2011; Mesmer-Magnus, Manapragada, Viswesvaran, & Allen, 2017). Thus, this study focuses on mindfulness as an important personality trait that may affect privacy attitudes and privacy decision making.

2.2 Privacy Disclosure

The impact of privacy concerns on various behavioural outcomes such as information disclosure, intention to transact online, willingness to pay or register with a website, has been well-documented (Smith et al., 2011). Among these, information disclosure has received most attention as a privacy decision outcome (Smith et al., 2011). Privacy disclosure refers to the communication of personal information, for example a person's name, phone number, home or email address, and other personal details to other entities in physical or digital environments (Mothersbaugh, Foxx, Beatty, & Wang, 2012), and relates to the type and level of information that individuals are willing to divulge with others (K. Li, Wang, Li, & Che, 2016). Studies have explored privacy disclosure decisions in various online environments such as social networking sites (Kroll & Stieglitz, 2019; K. Li et al., 2016), e-healthcare (Bansal, Zahedi, & Gefen, 2010), e-commerce (Anic, Škare, & Kursan Milaković, 2019), and online travel environments (Lu, Ioannou, Tussyadiah, & Li, 2019), demonstrating its critical role in shaping existing privacy research.

Recently, Gerber, Gerber and Volkamer (2018) concluded in their review that privacy concerns constitute one of the major determinants of disclosure attitudes and behaviours. The negative impact of privacy concerns on the intention to share personal information online has

been evidenced in various studies. Individuals with higher levels of privacy concerns are less willing to reveal information that are deemed personal and thus more likely to adopt privacy protection behaviours (Benamati et al., 2017). However, another stream of research, grounded on the premises of the 'privacy paradox' (Barth & De Jong, 2017), has argued the opposite. Although users reported to be very concerned about their online privacy and keen to protect their personal information, they did very little about it. Users voluntarily posted a great amount of details of their private life in SNS, used fitness trackers that record biometrics, or browsed various e-commerce websites that recorded behavioural data (e.g., searches conducted, content viewed) used for behavioural profiling (Gerber et al., 2018). Zafeiropoulou *et al.* (2013) confirmed that the privacy paradox exists in the case of location data where users do not act according with their stated privacy preferences and continue sharing their location with SNS (e.g., Facebook, Twitter). This study thus investigates information disclosure as the outcome of privacy concerns due to its relevance in privacy-related behaviour.

2.3 Protection Motivation Theory (PMT) and Privacy Threat Appraisal

Protection Motivation Theory (PMT) was firstly introduced in health research to explain risky health-related behaviours such as youth smoking and binge drinking (Youn, 2009). Building on the theory of fear appeals, PMT has been defined as using "persuasive messages designed to scare people by describing the terrible things that will happen to them if they do not do what the message recommends" (Witte, 1992, p. 329). The main contribution of PMT lies in predicting individuals' intentions to protect themselves after receiving such recommendations. At the core of PMT lies the idea that individuals' intentions and behaviours are influenced by two main cognitive processes when facing a threatening event: (1) threat appraisal and (2) cognitive appraisal (see Figure 1). Threat appraisal refers to one's evaluation of the severity as well as the vulnerability of the situation and threat, while cognitive appraisal refers to the evaluation of the actions that can remove the threat as well as the individual's abilities and competencies to cope with it.

One of the main premises of PMT is that there are two sources of information that can trigger this cognitive mediating process: environmental and intrapersonal sources (see Figure 1). Environmental sources include verbal persuasion and knowledge derived from observations, while intrapersonal sources refer to personality traits and feedback from prior experiences. These sources of information constitute the input variables in the model leading to the evaluation of the threat (i.e., threat and cognitive appraisals), ultimately resulting in an

action/response taken based on the information received (i.e., coping mode). The response can be either adaptive (i.e., to protect oneself) or not adaptive (i.e., not to protect oneself). In PMT, the result of the two cognitive processes is the individual's protection motivation (Crossler, 2010; Junglas et al., 2008). In this study, following PMT, mindfulness will be considered the personality trait and source of intrapersonal information that triggers the cognitive mediating process of an individual (see section 2.4).

[Figure 1 about here]

PMT is adopted in various information systems (IS) research, mostly to explore online safety and security behaviours and relevant motivations that can encourage protection of both individuals and organisations. For example, Hooper and Blunt, (2019) examined the factors that influence information security behavioural intentions of IT professionals while Visinescu *et al.* (2016) investigated the mechanisms in threat and coping appraisal processes that influence protection strategies of individuals using cloud computing storage services (Storage as a Service [STaaS]). Jansen and van Schaik (2018) examined how fear appeal messages might impact online information sharing behaviour showing their effectiveness in promoting security behaviours against phishing attacks. Williams, Nurse and Creese (2019) investigated the use of smartwatch games to encourage privacy protection behaviour in location tracking and sharing, app data collection and sharing, and stranger access. Finally, others examined the immediate and automatic reactions of technology users on context specific privacy threats (e.g., privacy breaches), revealing that their exposure led to limiting sensitive information disclosure and strengthening of passwords (Mamonov & Benbunan-Fich, 2018).

Applying PMT in the online privacy context, individual privacy concerns can be considered as a threat during the cognitive process that results in protection motivation that encourages risk-reducing behaviours. According to Junglas, Johnson and Spitzmüller (2008), a threat is perceived as the source of danger that can cause harm to an individual on a physical or mental level. Information privacy concerns can be considered as a threat to individuals as they are associated with feelings of fear and worry due to a potential privacy loss, invasion, or intrusion. More specifically, grounded on Smith, Milberg and Burke (1996)'s concern for information privacy (CFIP) instrument, privacy concerns regarding one's information disclosure involve several threats related to the collection, secondary use and sharing of personal information, as well as improper access from unauthorised entities, and errors in

storage of such information by organisations and service providers. Since PMT focuses on how individuals respond when receiving threatening information about situations they are engaging in, it can be inferred that in the context of privacy, the act of disclosure (i.e., providing personal sensitive information to online providers) can be a risky behaviour. According to Youn (2009), disclosure of sensitive personal information can be considered risky in the online context, as levels of privacy are associated with information risk relating to the uncertainty associated with data handling and sharing practices of online companies as well as the loss of control of personal information that might be used for unintended purposes. Loss of privacy can cause severe negative consequences to individuals ranging from emotional distress and anxiety, fear of monitoring, loss of anonymity to fraud and economic losses (Youn, 2009). Previous studies have adopted PMT in a similar vein, focusing on information disclosure behaviour such posting personal information in SNS (Marett, McNab, & Harris, 2011). This study employs PMT to understand individual tendencies to safeguard and prevent privacy losses caused by information collection, secondary use, and sharing practices by organisations and companies in online environments.

2.4 Mindfulness and Privacy Threat Appraisal

Mindfulness is defined as a receptive state of mind with open awareness, attention and perception of the present moment and experiences, beyond reactivity or judgment (Bergin & Pakenham, 2016; Schultz, Ryan, Niemiec, Legate, & Williams, 2015). Over the last three decades, studies have empirically shown the beneficial role of mindfulness in health and well-being outcomes such as decreasing depression, stress, and anxiety, enhancing well-being, as well as increasing emotional intelligence (Chiesa & Serretti, 2010). Research has depicted the concept of mindfulness either as a state (i.e., a momentary condition) or a dispositional trait (i.e., a stable characteristic) (Tomlinson et al., 2018). State mindfulness can be cultivated with various mindfulness interventions (e.g., mindfulness-based cognitive therapy [MBCT]), while dispositional (trait) mindfulness occurs naturally in different levels within people (Brown, Ryan, & Creswell, 2007). Recent evidence indicates that mindfulness training can increase trait mindfulness (Quaglia et al., 2016). This study focuses on dispositional (trait) mindfulness.

Mindfulness as a concept has received considerable attention in technology adoption and post-adoption behaviour studies (Jensen et al., 2017) as well as consumer behavior research (Ndubisi, 2014). Past research has investigated the effects of mindfulness on users' willingness to use a personal learning wiki system (Sun, Fang, Kong, & Kong, 2016) as well as developers'

intention to adopt existing software components (Stefi, 2015). Moreover, research has empirically shown the effectiveness of mindfulness in several areas: mitigating the negative consequences arising from information overload, such as users spending more time in order to identify and extract relevant information (Wolf, Pinter, & Beck, 2011), increasing academic performance in software engineering students (Bernárdez, Durán, Parejo, & Ruiz-Cortés, 2018), alleviating post-adoption regret arising from adopting herd behaviour in choosing amongst different wiki technologies (Zou, Sun, & Fang, 2015), reducing perceptions of technostress within the workplace while also improving user satisfaction and performance (Ioannou & Papazafeiropoulou, 2017) and, in the form of a training, decreasing people's vulnerability to phishing attacks (Jensen *et al.*, 2017).

This study argues that mindfulness, as a personality trait, is likely to have an important influence on privacy perceptions that will subsequently impact privacy protection behaviours. According to Wirth *et al.* (2017), individuals show differential levels of mindfulness during threat appraisal (e.g., identity theft) and coping appraisal (e.g., protection against identity theft). As a result, mindfulness levels will vary during these two cognitive processes. This study focuses on the influence of mindfulness on threat appraisal of privacy concerns. Following PMT, mindfulness is adopted as an intrapersonal source of information that triggers the cognitive mediating process of an individual.

2.5 Hypotheses Development

Research has argued that mindfulness facilitates more adaptive stress processing where more mindful people show a lower threat appraisal as they are able to interpret stressful events as more benign and less threatening (Weinstein, Brown, & Ryan, 2009). In more detail, in their study, Weinstein, Brown and Ryan, (2009) empirically demonstrated that mindfulness can reduce one's tendency to interpret situations as stress-inducing as more mindful individuals are using more adaptive strategies, such as active coping, acceptance, and cognitive reinterpretation of a situation.

In the context of privacy, privacy threats can be considered as stressors or stressful events; requests for personal information (e.g., face image, personal preferences) make one vulnerable to potential loss of privacy, which cause a wide range of negative consequences (Zimmer, Arsal, Al-Marzouq, & Grover, 2010). Adverse consequences of access and misuse of one's personal information can be physical, such as physical safety (e.g., stalking), psychological, such as a negative influence on one's well-being (e.g., mental discomfort), and social, such as negative changes in one's social relationships that impact an individual's status

in a social group (e.g., bullying, abuse) (Karwatzki, Trenz, Tuunainen, & Veit, 2017). Privacy concerns can be described as individuals worrying about their personal online privacy and the related potential misuse of personal, sensitive information from other entities or individuals. According to Delgado *et al.* (2010), worrying acts as an alarm warning about a potential upcoming danger (i.e., loss of privacy); worried thinking focuses on potential dangers and threats that might arise in the future. Evidence has shown that mindfulness can act as an antidote to worrying by promoting emotional and physiological regulatory mechanisms (Delgado et al., 2010).

There are several underlying mechanisms of mindfulness that can influence privacy threat appraisal during privacy decision making. At the core of mindfulness there are two fundamental components: (1) self-regulation of attention (awareness) of the present experience and (2) openness and acceptance of current experiences (Bishop et al., 2004). Mindfulness fosters awareness of the occurring stressors and threats, allowing one to stop habitual reactions of ineffective responding, taking a step back, and reacting non-judgementally (Alberts & Hülsheger, 2015). Being highly aware of present experiences, more mindful individuals are more likely to consider the factors that may harm one's sense of privacy more objectively and evaluate their effect in certain situation or environment (i.e., losing control of personal information), the severity of the privacy threat, as well as their own (self) vulnerability to the threat. In accordance with PMT, this will allow individuals to make more balanced decisions, avoiding habitual reactivity and judgement. Also, mindfulness by definition encompasses the state of acceptance, being experientially open to present moments, as "… an active process in that the [individual] chooses to take what is offered with an attitude of openness and receptivity to whatever happens to occur in the field of awareness" (Bishop et al., 2004, p. 233). Therefore, more mindful people are more likely to accept the occurring threat as well as their own vulnerability, thus being able to maintain a peace of mind and feel less fear or worry over occurring threats. Furthermore, recent evidence indicates that two of the central mechanisms of mindfulness, observing (awareness of present moment) and acceptance, are associated with less threat appraisals resulting in lower stress levels (Hoffmann & Geisler, 2020).

Moreover, another key element of mindfulness is decoupling (decentering), describing the ability of an individual to distance or separate oneself from negative experiences, thoughts and emotions allowing for positive appraisal (Glomb, Duffy, Bono, & Yang, 2011); a more mindful person is more likely to observe stressors less emotionally, evaluate them in more benign or neutral terms, and therefore show less negative and more positive reactions (Good et al., 2016). In their study using functional neuroimaging, Creswell *et al.* (2007) showed a greater

prefrontal cortal activity and concomitant inhibition of the limbic system in individuals with high dispositional mindfulness (trait), indicating a decrease in automatic affective responses. This suggests that mindfulness can potentially reduce negative affect and enhance one's ability to monitor one's own emotional state.

Concentrating on the present moment and experiences and making an effort to think before habitually reacting during unsettling situations that might involve loss of privacy, a more mindful person is more likely to judge such situations as less harming and respond more objectively to privacy threats. According to Langer (2014) mindfulness fosters one's ability to perceive stressors in certain situations as challenges rather than as threats. Mindfulness fosters acceptance, allowing reinterpretation of a worrying situation, where a privacy threat is more likely to be interpreted as an opportunity to learn something new rather than as a harmful situation. For example, when installing a new application on a smartphone, providers usually request access to the user's address book (e.g., list of contacts), camera, and microphone that might trigger individual concerns over privacy. A more mindful user is more likely to consider this situation as a learning experience, taking a step back before deciding on which options to select, evaluating the benefits, drawbacks, and potential alignment with internal goals and values (Karelaia & Reb, 2015).

Overall, through the above underlying mechanisms of mindfulness we expect that more mindful individuals are more likely to react less emotionally and more objectively upon privacy threats; evaluate them as more neutral and benign, showing more positive and less negative reactions during threat appraisal, thus showing lower levels of privacy concerns. Therefore, we hypothesize that:

H1: Mindfulness is negatively associated with privacy concerns

Prior research has identified privacy concerns as a major predictor of information disclosure (Gerber et al., 2018); individuals expressing higher concerns related to their privacy are more unwilling to share personal information with online providers. The act of sharing private sensitive data with online providers constitutes a risky behaviour, thus, grounded on existing literature, we predict that higher privacy concerns will result in lower intention to share personal data online. This leads to the following hypothesis:

H2: Privacy concerns are negatively associated with willingness to share information

Overall, the research hypotheses and proposed theoretical model are presented in Figure 2. Previous research has shown that other individual variables such as demographic factors may influence privacy concerns as well as one's willingness to disclose information with online companies (Y. Li, 2011; Wakefield, 2013). In order to rule out such confounding effects, age,

gender, and levels of education will be integrated into the proposed theoretical model as control variables.

[Figure 2 about here]

3. Method

An online survey was distributed in May 2019 as a part of a project investigating consumer attitudes towards privacy and data sharing in online travel environments. A professional research company was used in order to administer the questionnaire to a panel of residents in the United Kingdom. All measures have been adopted from existing literature. The construct of privacy concerns was adapted from existing studies in privacy literature with a 5-point scale (1 = "Strongly disagree" – 5 = "Strongly agree") (Smith, Milberg, & Burke, 1996; Xu, Dinev, Smith, & Hart, 2011;Wozniak, Schaffner, Stanoevska-Slabeva, & Lenz-Kesekamp, 2018). For the construct of mindfulness, the most widely used instrument for the measurement of dispositional mindfulness, referred as MAAS (Brown & Ryan, 2003), with a 6-point scale (1 = "Almost never" – 6 = "Almost always") was used. The construct of willingness to share personal information online was self-developed with a 5-point scale. More details on the constructs and their items are presented in Appendix B. Moreover, demographic information was requested from participants regarding age, gender (0 = male, 1 = female), highest levels of education, employment status, and online shopping experience.

Overall, 836 responses were obtained. The preliminary screening of data, removing missing data, determined that the usable sample size is 685. Of these, 359 (53%) were female, showing almost balanced gender representation. Most of the participants were between the ages of 26-65, with almost equal representantion in the second and fifth age groups (e.g., 25-35: 24%, 56-65:22%). Most respondents have achieved at least high school education, with the largest groups being high school education (39%), followed by Bachelor degree (35%). Most respondents work in the private sector (37.2%), followed by retirement (25.3%), while the majority of them shop online several times a month (41.3%).

[Table 1 about here]

This study conducted covariance based structural equation modeling (CB-SEM) using AMOS 25 in order to analyse the collected data. Exploratory factor analysis (EFA) was used in order to discover the underlying factor structure of the latent variable Willingness to Share Information (see Appendix A); while confirmatory factor analysis (CFA) was performed in evaluate the reliability, convergent and discriminant validity of the measurement model. Finally, the structural model was evaluated and the proposed hypotheses were tested, examining also the indirect relationship between mindfulness and information disclosure intention.

4. Results

4.1 Common Method Bias

This study performed several tests to check for the existence of common method bias (CMV) (Mackenzie, Podsakoff, & Podsakoff, 2011; Podsakoff, MacKenzie, Lee, & Podsakoff, 2003). First, we conducted Harman's one-factor test yielding a cumulative 20% of variance thus indicating that common method bias is not evident in this study. An additional test was implemented following the method proposed by Pavlou, Liang and Xue, (2007) ensuring that correlations do not exceed 0.90. The results revealed that all correlations are lower than the cut-off threshold (see Appendix A). A multicollinearity test showed that VIFs were lower than the suggested cut-off of 3.3 (Pallant, 2010) for the independent variables of the model (see Appendix A). Overall, we can conclude that common method bias does not pose significant concern in this study.

4.2 Structural Equation Modeling

During CFA, few items with inadequate factor loadings (< 0.5) were not retained in the final model (see Table A4 in Appendix A). Relevant tests regarding reliability and validity were estimated. Evaluation of composite reliability (CR), average variance extracted (AVE), was undertaken by checking against cut-off criteria: AVE values should exceed the recommended threshold of 0.50, and CR values should exceed 0.70 (Hair, Black, Babin, Anderson, and Tatham, 2010). Results suggest that convergent validity and construct reliability have been established. Discriminant validity was evaluated to ensure that the square root of variance shared between constructs is larger than the correlation between the construct and other variables (Fornell & Larcker, 1981) (see Tables 2-3). The goodness-of-fit indices both

for CFA and structural model suggest that there is good fit of the data in the proposed model (Hair et al., 2010) (see Table 3). Figure 3 presents the means of participants' willingness to dislose different types of personal information.

[Table 2 about here]

[Table 3 about here]

[Figure 3 about here]

Results from the structural model showed that all hypotheses are confirmed (see Figure 4 and Table 4). More specifically, the analysis showed that more mindful individuals have lower privacy concerns (b= -0.216, $p < 0.001$), while individuals with higher privacy concerns are less willing to disclose personal information to online companies (b= -0.077, $p < 0.05$). Also, the analysis showed that the integration of the control variables in the model, gender (b= -0.089, $p < 0.05$) and age (b= -0.117, $p < 0.05$) have a significant negative impact on willingness to share information, while education showed no significant impact. Also, age showed a significant positive association with privacy concerns (b= 0.097, $p < 0.05$).

[Figure 4 about here]

[Table 4 about here]

We also tested for the indirect effect of mindfulness on willingness to share information, since the relationship is mediated by privacy concerns. Results show that privacy concerns partially mediate the effect of mindfulness on willingness to share information (b= 0.021, p= 0.009), while there is a direct negative effect of mindfulness on willingness to share information (b= -0.174, $p < 0.001$) resulting in a total negative effect (b= -0.153, $p < 0.001$) (see Table 5).

[Table 5 about here]

5. Discussion

Evidence shows that almost 79% of individuals report concerned about sharing their personal information online (Auxier & Rainie, 2019), thus experiencing mental discomfort regarding their online privacy. Therefore, privacy concerns can be considered a threat, where the individual experiences feelings of stress, fear, and worry in sight of potential loss of control of

personal information that can result in several 'harmful' consequences such as privacy invasion, identity theft, as well as financial and social losses (Karwatzki et al., 2017). This study focuses on the role of mindfulness, as a personality trait, as a determinant of privacy concerns during threat appraisal. By adopting PMT, this study examines the influence of mindfulness on privacy concerns to better understand whether mindfulness can affect privacy attitudes, thus indirectly influencing consumer privacy decision making.

Our findings reveal that mindfulness as a personality trait is influential in the formation of privacy concerns, with more mindful individuals showing lower privacy concerns. In agreement with existing research suggesting that mindfulness can foster more adaptive stress processing where more mindful people show a lower threat appraisal as they are able to re-interpret stressful events (threats) as more benign and less threatening (Weinstein, Brown and Ryan, 2009), our findings demonstrate that a more mindful individual is more likely to adopt a more objective appraisal style, thus interpreting privacy threats as less threatening. More mindful people are able to disengage from an initial negative appraisal and emotional reaction, taking a step back (Garland, Gaylord, & Fredrickson, 2011), and thus being more resilient than others as they perceive stressful events as more manageable and are able to respond more flexibly (Schultz et al., 2015).

6. Implications to Research and Practice

6.1 Theoretical Implications

Our findings offer important theoretical implications. First, this work expands extant privacy literature on the antecedents of information privacy concerns by explaining the role of individual differences, specifically mindfulness, in forming consumer privacy attitudes and privacy behaviour (Egelman & Peer, 2015b; Junglas et al., 2008; Smith et al., 2011). Our findings reveal the influential role of mindfulness as a personality trait on privacy concerns and thus its indirect influence on privacy behaviour. Our results come in accordance with recent evidence suggesting that central tenets of mindfulness, observing individual's own experiences with acceptance, can lessen threat appraisals of demands; suggesting that through these processes mindfulness is associated with lower levels of perceived stress, thus contributing to enhanced well-being (Hoffmann & Geisler, 2020). Also, this study enhances IS and mindfulness literature by empirically examining the concept from a privacy perspective, using the lens of PMT. Although previous studies have investigated the concept of mindfulness

during threat and coping assessment in various contexts involving stress (Weinstein et al., 2009), this is one of the first studies to empirically investigate the impact of trait mindfulness on individuals' concerns during threat appraisal and privacy disclosure in the online privacy context.

Moreover, our findings provide a theoretical foundation to explain the formation of privacy behaviours as a result of individual differences offering a perspective on how mindfulness may impact certain online disclosure decisions. Our study confirms that privacy concerns mediate the relationship between mindfulness and information disclosure, suggesting that more mindful consumers show lower concerns over their online privacy, and are willing to share their personal information with online travel providers. Nascent mindfulness research suggests that mindfulness can help people in decision making resulting in high quality decisions, by allowing cognitive processing without impulsive reactions to immediate needs (Karelaia & Reb, 2015). More mindful individuals are more aware of their internal values, goals and needs, thus are more likely to respond to occurring situations by striving to fulfil their fundamental objectives (Karelaia & Reb, 2015). Thus, the disclosure decisions of more mindful participants in this study may be aligned with their own internal values and goals. Furthermore, in recent research focusing on deploying mindfulness to avoid phishing attacks, Jensen et al. (2017) argue that since mindfulness fosters pausing to consider the present context before acting, it enables greater receptive attention allowing individuals to identify critical details as well as the reasonableness of requests, enabling them to distinguish between phishing and legitimate message requests. By forestalling judgement, mindfulness enables individuals to attend to and not suppress suspicion, reducing mindless acceptance and processing of occurring requests (Jensen et al., 2017). More mindful people pay extraordinary attention to the present moment, seeing more connections in events, actions and thoughts taking place, and thus are more likely to identify false patterns (Karelaia & Reb, 2015). Mindfulness fosters active questioning about the context and the implications of one's actions; "If you ask questions that encourage mindfulness, you bring people to the present and you're more likely to avoid an accident" (Langer, 2014, p. 72). Therefore, in our sample, more mindful individuals may evaluate the reasonableness as well as consequences of information sharing in the present context (i.e., online travel environment); thoughtfully considering what is a better decision for oneself (e.g., share personal information with online providers) by pausing and reflecting, escaping mindless processing and emotional reactions (e.g., oversharing or refusing disclosure) to occurring privacy threats, hence showing higher intention towards information disclosure.

For example, when faced with a request such as sharing one's fingerprint information with an online travel provider in order to speed up the boarding procedure, a more mindful consumer is more likely to consider the consequences of such decision and accept the sharing request by evaluating the reasonableness of such request.

Interestingly, contrary to our initial assumption, our results suggest that more mindful participants may not associate the specific act of disclosure as risky in this specific context (i.e., online travel). Indeed, past research argues that privacy decision making is a highly context dependent phenomenon; on some occasions people are reluctant to share their personal information while in other situations they show complete apathy (Acquisti, Brandimarte, & Loewenstein, 2015). Future studies are imperative in this area of research, in order to examine the association of mindfulness, privacy concerns and intention to disclose information in different contexts, such as e-commerce, e-healthcare, and different types of sensitive personal information (e.g., financial information, health-related information) as they might yield differential results. Overall, our study contributes to existing literature by offering empirical evidence supporting the potential linkages between mindfulness and information disclosure, serving as the a foundation for future research to exploring this relationship in more depth.

Furthermore, it is important to note that the mediation analysis (i.e., through privacy concerns) resulted in a negative direct effect, a positive indirect effect, and a total negative effect of mindfulness on information disclosure; indicating that the role of mindfulness in influencing this privacy outcome is rather complex and hence demands further investigation. Our results (i.e., partial mediation) suggest that there are other confounding processes and factors that might influence the relationship of mindfulness and information disclosure. In this study, there might be other factors – other than personality traits - that affect privacy decision making - along with mindfulness. According to Acquisti et al. (2017), online privacy decisions are influenced by cognitive and behavioural biases, such as anchoring and overconfidence, emotions and mental shortcuts. Interestingly, recent evidence suggests that mindfulness, fostering awareness of present context and possibilities, can increase rationality in decisions, improving decision making by reducing most cognitive biases (e.g., overconfidence, confirmation bias, availability bias and anchoring) (Maymin & Langer, 2021). Future research is essential to further investigate the role of mindfulness in privacy decision making.

6.2 Practical Implications

This study offers important implications for practice. Understanding more comprehensively the various factors that influence the formation of privacy attitudes can assist in identifying and developing ways to assist and support individual privacy decision making. At first, our findings will bring awareness to marketers and practitioners about the important role of users' characteristics in influencing privacy attitudes and behaviour. Instead of implementing one-size-fits-all approaches to privacy enhancing and protection mechanisms, they should be designed and developed based on salient dispositional factors of consumers in order to strengthen trust and feelings of ease when requesting such information sharing. For example, the provision of clear and transparent privacy statements and policies from companies' websites has been suggested to increase privacy assurance for users who might be more worried and fearful of privacy invasions, strengthening their trust with the online provider and thus increasing their willingness to share personal information (Bhatia, Breaux, Reidenberg, & Norton, 2016; Hui, Teo, & Lee, 2007). Moreover, our findings highlight the importance of fostering individual mindfulness that can help consumers in lowering threat appraisals of occurring demands during privacy decision making that can reduce stress and contribute to enhanced well-being. As a malleable trait, mindfulness is an easily taught tool can be enhanced through a wide range of practices and techniques that consumers can adopt, such as mindfulness-based interventions and/or digital mindfulness platforms and applications, with flexible implementations ranging from an 8-week intervention program to five minutes a day practice (Good et al., 2016; Mrazek et al., 2019).

7. Conclusions, Limitations and Future Work

The present study examines the influence of dispositional mindfulness, an important personality trait, on the formation of privacy concerns and intention to share personal information in an online travel context, through the lens of protection motivation theory (PMT), aiming to serve as the foundation for future studies in this important area of research. Using an online survey with responses from 685 UK-based individuals and SEM to test the proposed hypotheses, the study demonstrates the paramount role of mindfulness in people's threat appraisal process of privacy concerns, and the subsequent impact on information disclosure. A more mindful consumer shows less privacy concerns and is more likely to adopt a more objective appraisal style, interpret privacy threats as less threatening, sharing personal information online.

In this study, a sample of 685 individuals was recruited from the UK. Future research should attempt to replicate our results in other populations such as consumers working in specific industries (e.g., IT) and different cultures (e.g., Asia). Moreover, mindfulness was adopted as the only personality trait affecting privacy concerns in this study. However, as individuals are characterised with several different traits, it would be important for future research to investigate other personality differences in conjunction with mindfulness as covariates in order to understand the differential impact of each of the constructs on privacy concerns and information disclosure. Also, this study employed an online survey to examine the impact of privacy concerns on self-reported measures of disclosure intention. Although most empirical privacy research has used intention as a determinant of actual disclosure, the mere existence of the privacy paradox demands further research. Future studies should conduct experimental studies in real settings in order to measure mindfulness levels as well as concerns and actual disclosure behaviours of individuals. Lastly, investigating mindfulness in a privacy context has been an under-researched area; more studies are essential in order to understand in more depth the association of mindfulness with privacy attitudes and privacy behaviours. Since our results are quantitative, it is important for further research to conduct qualitative studies (e.g., through interviews or focus groups) in order to confirm our results as well as explore in a more comprehensive manner the underlying mechanisms of mindfulness that people deploy during privacy threats and appraisal.

References

Acquisti, A., Adjerid, I., Balebako, R. H., Brandimarte, L., Cranor, L. F., Komanduri, S., … Wilson, S. (2017). Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online. *ACM Computing Surveys*, *50*(3). https://doi.org/10.2139/ssrn.2859227

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509–514.

Aivazpour, Z., & Rao, V. S. (Chino). (2019). Impulsivity and Information Disclosure: Implications for Privacy Paradox. *Proceedings of the 52nd Hawaii International Conference on System Sciences*, *6*, 4861–4874. https://doi.org/10.24251/hicss.2019.586

Alberts, H. J. E. M., & Hülsheger, U. R. (2015). Applying mindfulness in the context of work: mindfulness based interventions. In J. Reb & P. W. B. Atkins (Eds.), *Mindfulness in Organizations: Foundations, Reseach and Applications* (pp. 100–132). Cambridge University Press.

Alohali, M., Clarke, N., Li, F., & Furnell, S. (2018). Identifying and predicting the factors affecting end-users' risk-taking behavior. *Information and Computer Security*, *26*(3), 306–326. https://doi.org/10.1108/ICS-03-2018-0037

Anic, I. D., Škare, V., & Kursan Milaković, I. (2019). The determinants and effects of online privacy concerns in the context of e-commerce. *Electronic Commerce Research and Applications*. https://doi.org/10.1016/j.elerap.2019.100868

Auxier, B., & Rainie, L. (2019). *Americans' views about privacy, surveillance and data-sharing*. Retrieved from https://www.pewresearch.org/fact-tank/2019/11/15/key-takeaways-on-americans-views-about-privacy-surveillance-and-data-sharing/

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

Barth, S., & De Jong, M. D. T. (2017). The privacy paradox–Investigating discrepancies between expressed privacy concerns and actual online behavior–A systematic literature review. *Telematics and Informatics*, *34*(7), 1038–1058.

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online Privacy Concerns and Privacy Management: A Meta-Analytical Review. *Journal of Communication*, *67*(1), 26–53. https://doi.org/10.1111/jcom.12276

Benamati, J. H., Ozdemir, Z. D., & Smith, H. J. (2017). An empirical test of an Antecedents - Privacy Concerns - Outcomes model. *Journal of Information Science*, *43*(5), 583–600. https://doi.org/10.1177/0165551516653590

Bergin, A. J., & Pakenham, K. I. (2016). The Stress-Buffering Role of Mindfulness in the Relationship Between Perceived Stress and Psychological Adjustment. *Mindfulness*, *7*(4), 928–939. https://doi.org/10.1007/s12671-016-0532-x

Bernárdez, B., Durán, A., Parejo, J. A., & Ruiz-Cortés, A. (2018). An experimental replication on the effect of the practice of mindfulness in conceptual modeling performance. *Journal of Systems and Software*, *136*, 153–172. https://doi.org/10.1016/j.jss.2016.06.104

Bhatia, J., Breaux, T. D., Reidenberg, J. R., & Norton, T. B. (2016). A Theory of Vagueness and Privacy Risk Perception. *2016 IEEE 24th International Requirements Engineering Conference*, 26–35. https://doi.org/10.1109/RE.2016.20

Bishop, S., Lau, M., Shapiro, S., Carlson, L., Anderson, N., Carmody, J., … Devins, G. (2004). Mindfulness: A Proposed Operational Definition. *Clinical Psychology: Science and Practice*,

11(3), p.230. https://doi.org/10.1093/clipsy/bph077

Bradely, R. (2019). Data Privacy Concerns: An Overview for 2019. *Medium*. Retrieved from https://medium.com/@the_manifest/data-privacy-concerns-an-overview-for-2019-2ccea79aa6f8

Brown, K. W., & Ryan, R. M. (2003). The benefits of being present: mindfulness and its role in psychological well-being. *Journal of Personality and Social Psychology*, *84*(4), 822–848. https://doi.org/10.1037/0022-3514.84.4.822

Brown, K. W., Ryan, R. M., & Creswell, J. D. (2007). Mindfulness: Theoretical Foundations and Evidence for its Salutary Effects. *Psychological Inquiry*, *18*(4), 211–237. https://doi.org/10.1080/10478400701598298

Chiesa, A., & Serretti, A. (2010). A systematic review of neurobiological and clinical features of mindfulness meditations. *Psychological Medicine*, *40*(8), 1239–1252. https://doi.org/10.1017/S0033291709991747

Creswell, J. D., Way, B. M., Eisenberger, N. I., & Lieberman, M. D. (2007). Neural correlates of dispositional mindfulness during affect labeling. *Psychosomatic Medicine*, *69*(6), 560–565. https://doi.org/10.1097/PSY.0b013e3180f6171f

Crossler, R. E. (2010). Protection motivation theory: Understanding determinants to backing up personal data. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 1–10. https://doi.org/10.1109/HICSS.2010.311

Davis, D. M., & Hayes, J. a. (2011). What are the benefits of mindfulness? A practice review of psychotherapy-related research. *Psychotherapy (Chicago, Ill.)*, *48*(2), 198–208. https://doi.org/10.1037/a0022062

Delgado, L. C., Guerra, P., Perakakis, P., Vera, M. N., del Paso, G. R., & Vila, J. (2010). Treating chronic worry: Psychological and physiological effects of a training programme based on mindfulness. *Behaviour Research and Therapy*, *48*(9), 873–882. https://doi.org/10.1016/j.brat.2010.05.012

Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents -measurement validity and a regression model. *Behaviour and Information Technology*, *23*(6), 413–422. https://doi.org/10.1080/01449290410001715723

Dinev, T., & Hart, P. (2006). Internet Privacy Concerns and Social Awareness as Determinants of Intention to Transact. *International Journal of Electronic Commerce*, *10*(2), 7–29. https://doi.org/10.2753/JEC1086-4415100201

Egelman, S., & Peer, E. (2015a). Predicting privacy and security attitudes. *ACM SIGCAS Computers and Society*, *45*(1), 22–28. https://doi.org/10.1145/2738210.2738215

Egelman, S., & Peer, E. (2015b). The Myth of the Average User: Improving Privacy and Security Systems through Individualization. *Proceedings of the New Security Paradigms Workshop on ZZZ - NSPW '15*, 16–28. https://doi.org/10.1145/2841113.2841115

Floyd, D., Prentice-Dunn, S., & Rogers, R. (2000). A Meta-Analysis of Research on Protection Motivation Theory. *Journal of Applied Psychology*, *30*(2), 407–429.

Fornell, C., & Larcker, D. F. (1981). Structural Equation Models with Unobservable Variables and Measurement Error: Algebra and Statistics. *Journal of Marketing Research*, *18*(3), 382–388. https://doi.org/10.1177/002224378101800313

Garland, E. L., Gaylord, S. A., & Fredrickson, B. L. (2011). Positive Reappraisal Mediates the Stress-Reductive Effects of Mindfulness: An Upward Spiral Process. *Mindfulness*, *2*(1), 59–67. https://doi.org/10.1007/s12671-011-0043-8

Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review

of literature investigating privacy attitude and behavior. *Computers and Security*. https://doi.org/10.1016/j.cose.2018.04.002

Glomb, T. M., Duffy, M. K., Bono, J. E., & Yang, T. (2011). Mindfulness at Work. *Research in Personnel and Human Resources Management*, *30*, 115–157. https://doi.org/10.1108/S0742-7301(2011)0000030005

Good, D. J., Lyddy, C. J., Glomb, T. M., Bono, J. E., Brown, K. W., Duffy, M. K., … Lazar, S. W. (2016). Contemplating Mindfulness at Work: An Integrative Review. *Journal of Management*, *42*(1), 114–142. https://doi.org/10.1177/0149206315617003

Hair, J. F., Black, W., Babin, B., Anderson, R., & Tatham, R. (2010). *Multivariate data analysis* (6th ed.). Pearson Prentice Hall.

Heravi, A., Mubarak, S., & Raymond Choo, K. K. (2018). Information privacy in online social networks: Uses and gratification perspective. *Computers in Human Behavior*, *84*, 441–459. https://doi.org/10.1016/j.chb.2018.03.016

Hoffmann, C. F. A., & Geisler, F. C. M. (2020). Accept what you observe: A conditional process model linking mindfulness facets, threat appraisal, and perceived stress in German college students. *Personality and Individual Differences*, *156*(July 2019), 1–5. https://doi.org/10.1016/j.paid.2019.109752

Hooper, V., & Blunt, C. (2019). Factors influencing the information security behaviour of IT employees. *Behaviour and Information Technology*, *39*(8), 862–874. https://doi.org/10.1080/0144929X.2019.1623322

Hui, K., Teo, H., & Lee, S. (2007). The Value of Privacy Assurance: An Exploratory Field Experiment. *MIS Quarterly*, *31*(1), 19–33. https://doi.org/10.2307/25148779

Ioannou, A., & Papazafeiropoulou, A. (2017). Using it mindfulness to mitigate the negative consequences of technostress. *AMCIS 2017 - America's Conference on Information Systems: A Tradition of Innovation*, *2017-Augus*.

Jansen, J., & van Schaik, P. (2018). Design and Evaluation of a Theory-Based Intervention To Promote Security Behaviour Against Phishing. *International Journal of Human-Computer Studies*. https://doi.org/10.1016/j.ijhcs.2018.10.004

Jensen, M. L., Dinger, M., Wright, R. T., & Thatcher, J. B. (2017). Training to Mitigate Phishing Attacks Using Mindfulness Techniques. *Journal of Management Information Systems*, *34*(2), 597–626. https://doi.org/10.1080/07421222.2017.1334499

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

Karelaia, N., & Reb, J. (2015). Improving decision making through mindfulness. In Jochen Reb & P. Atkins (Eds.), *Mindfulness in Organizations: Foundations, Reseach and Applications* (pp. 163–189). Cambridge University Press.

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

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

Kroll, T., & Stieglitz, S. (2019). Digital nudging and privacy: improving decisions about self-

disclosure in social networks *. *Behaviour and Information Technology*, *0*(0), 1–19. https://doi.org/10.1080/0144929X.2019.1584644

Langer, E. (2014). Mindfulness in the age of complexity. *Harvard Business Review*, *92*(3), 68–73.

Li, K., Wang, X., Li, K., & Che, J. (2016). Information privacy disclosure on social network sites: An empirical investigation from social exchange perspective. *Nankai Business Review International*, *7*(3), 282–300. https://doi.org/10.1108/NBRI-02-2015-0005

Li, P., Cho, H., & Goh, Z. H. (2019). Unpacking the process of privacy management and self-disclosure from the perspectives of regulatory focus and privacy calculus. *Telematics and Informatics*. https://doi.org/10.1016/j.tele.2019.04.006

Li, Y. (2011). Empirical Studies on Online Information Privacy Concerns: Literature Review and an Integrative Framework. *Communications of the Association for Information Systems*, *28*(28), 453–496. https://doi.org/http://aisel.aisnet.org/cais/vol28/iss1/28

Liang, H., Saraf, N., Hu, Q., & Xue, Y. (2007). Assimilation of enterprise systems: The effect of institutional pressures and the mediating role of top management. *MIS Quarterly: Management Information Systems*, *31*(1), 59–87. https://doi.org/10.2307/25148781

Lu, Y., Ioannou, A., Tussyadiah, I., & Li, S. (2019). Segmenting Travelers Based on Responses to Nudging for Information Disclosure. *E-Review of Tourism Research*, *17*(3), 394–406.

Mackenzie, S. B., Podsakoff, P. M., & Podsakoff, N. P. (2011). Construct Measurement and Validation Procedures in MIS and Behavioral Research : Integrating New and Existing Techniques. *MIS Quarterly*, *35*(2), 293–334. https://doi.org/10.2307/23044045

Mamonov, S., & Benbunan-Fich, R. (2018). The impact of information security threat awareness on privacy-protective behaviors. *Computers in Human Behavior*, *83*, 32–44. https://doi.org/10.1016/j.chb.2018.01.028

MAPPG. (2015). Mindful Nation UK. In *The Mindfulness All-Party Parlamentary Group*. Retrieved from http://www.themindfulnessinitiative.org.uk/images/reports/Mindfulness-APPG-Report_Mindful-Nation-UK_Oct2015.pdf

Marett, K., McNab, A., & Harris, R. (2011). Social Networking Websites and Posting Personal Information: An Evaluation of Protection Motivation Theory. *AIS Transactions on Human-Computer Interaction*, *3*(3), 170–188. https://doi.org/10.17705/1thci.00032

Maymin, P. Z., & Langer, E. J. (2021). Cognitive biases and mindfulness. *Humanities and Social Sciences Communications*, *8*(1). https://doi.org/10.1057/s41599-021-00712-1

Mesmer-Magnus, J., Manapragada, A., Viswesvaran, C., & Allen, J. W. (2017). Trait mindfulness at work: A meta-analysis of the personal and professional correlates of trait mindfulness. *Human Performance*, *30*(2–3), 79–98. https://doi.org/10.1080/08959285.2017.1307842

Mirsch, T., Lehrer, C., & Jung, R. (2017). Digital Nudging: Altering User Behavior in Digital Environments. *Wirtschaftsinformatik 2017*, (February), 634–648.

Mothersbaugh, D. L., Foxx, W. K., Beatty, S. E., & Wang, S. (2012). Disclosure Antecedents in an Online Service Context: The Role of Sensitivity of Information. *Journal of Service Research*, *15*(1), 76–98. https://doi.org/10.1177/1094670511424924

Mrazek, A. J., Mrazek, M. D., Cherolini, C. M., Cloughesy, J. N., Cynman, D. J., Gougis, L. J., … Schooler, J. W. (2019). The future of mindfulness training is digital, and the future is now. *Current Opinion in Psychology*, *28*, 81–86. https://doi.org/10.1016/j.copsyc.2018.11.012

Ndubisi, N. (2014). Consumer Mindfulness and Marketing Implications. *Psychology & Marketing*, *31*(4), 237–250. https://doi.org/10.1002/mar.20691

Osatuyi, B. (2015). Personality Traits and Information Privacy Concern on Social Media Platforms. *The Journal of Computer Information Systems*, *55*(4), 11–19. https://doi.org/10.1080/08874417.2015.11645782

Pallant, J. (2010). *SPSS survival manual : a step by step guide to data analysis using SPSS*. Open University Press/McGraw-Hill.

Pavlou, P. (2011). State of the Information Privacy Literature: Where Are We Now and Where Should We Go? *MIS Quarterly*, *35*(4), 1063–1078.

Pavlou, P., Liang, H., & Xue, Y. (2007). Understanding And Mitigating Uncertainty In Online Exchange Relationships: A principal Agent Perspective. *MIS Quarterly*, *31*(1), 105–136.

Podsakoff, P. M., 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. https://doi.org/10.1037/0021-9010.88.5.879

Quaglia, J. T., Braun, S. E., Freeman, S. P., Mcdaniel, M. A., Brown, K. W., Quaglia, J. T., … Brown, K. W. (2016). Meta-Analytic Evidence for Effects of Mindfulness Training on Dimensions of Self-Reported Dispositional Mindfulness. *Psychological Assessment*, *28*(7), 803–818. https://doi.org/10.1037/pas0000268

Rogers, R. D. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, *91*, 93–114.

Schultz, P. P., Ryan, R. M., Niemiec, C. P., Legate, N., & Williams, G. C. (2015). Mindfulness, Work Climate, and Psychological Need Satisfaction in Employee Well-being. *Mindfulness*, *6*(5), 971–985. https://doi.org/10.1007/s12671-014-0338-7

Smith, H. J., Dinev, T., & Xu, H. (2011). Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly*, *35*(4), 1063–1078. https://doi.org/10.2307/41409970

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *MIS Quarterly*, *20*(2), 167. https://doi.org/10.2307/249477

Stefi, A. (2015). Do Developers Make Unbiased Decisions - The Effect of Mindfulness. *Twenty-Third European Conference on Information Systems (ECIS), Münster, Germany, 2015*, 1–15.

Sun, H., Fang, Y., Kong, H., & Kong, H. (2016). Choosing a Fit Technology: Understanding Mindfulness in Technology Adoption and Continuance. *Journal of the Association for Information Systems*, *17*(6), 377–412.

Tomlinson, E. R., Yousaf, O., Vittersø, A. D., & Jones, L. (2018, February 1). Dispositional Mindfulness and Psychological Health: a Systematic Review. *Mindfulness*, Vol. 9, pp. 23–43. https://doi.org/10.1007/s12671-017-0762-6

Van Dam, N. T., van Vugt, M. K., Vago, D. R., Schmalzl, L., Saron, C. D., Olendzki, A., … Meyer, D. E. (2018). Mind the Hype: A Critical Evaluation and Prescriptive Agenda for Research on Mindfulness and Meditation. *Perspectives on Psychological Science*, *13*(1), 36–61. https://doi.org/10.1177/1745691617709589

Visinescu, L. L., Azogu, O., Ryan, S. D., Wu, Y., & Kim, D. J. (2016). Better Safe than Sorry: A Study of Investigating Individuals' Protection of Privacy in the Use of Storage as a Cloud Computing Service. *International Journal of Human-Computer Interaction*, *32*(11), 885–900. https://doi.org/10.1080/10447318.2016.1204838

Wakefield, R. (2013). The influence of user affect in online information disclosure. *Journal of Strategic Information Systems*. https://doi.org/10.1016/j.jsis.2013.01.003

Weinstein, N., Brown, K. W., & Ryan, R. M. (2009). A multi-method examination of the effects of

mindfulness on stress attribution, coping, and emotional well-being. *Journal of Research in Personality*, *43*(3), 374–385. https://doi.org/10.1016/j.jrp.2008.12.008

Williams, M., Nurse, J. R. C., & Creese, S. (2019). Smartwatch games: Encouraging privacy-protective behaviour in a longitudinal study. *Computers in Human Behavior*, *99*, 38–54. https://doi.org/10.1016/j.chb.2019.04.026

Wirth, J., Laumer, S., Maier, C., & Weitzel, T. (2017). Understanding Privacy Threat Appraisal and Coping Appraisal through Mindfulness. *ICIS 2017 Proceedings*, 1–11.

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communication Monographs*, *59*(4), 329–349. https://doi.org/10.1080/03637759209376276

Wolf, M., Pinter, T., & Beck, R. (2011). Individual Mindfulness and It Systems Use - Mitigating Negative Consequences of Information Overload. *ECIS 2011*, 1–13.

Yao, M., Rice, R., & Wallis, K. (2007). Predicting User Concerns About Online Privacy. *Journal of the Americal Society for Information Science and Technology*, *58*(5), 710–722. https://doi.org/10.1002/asi

Yeh, C., Wang, Y.-S., Lin, S.-J., Tseng, T. H., Lin, H.-H., Shih, Y.-W., & Lai, Y.-H. (2018). What drives internet users' willingness to provide personal information? *Online Information Review*, *42*(6), 923–939. https://doi.org/10.1108/OIR-09-2016-0264

Youn, S. (2009). Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors Among Young Adolescents. *The Journal of Consumer Affairs*, *43*(3), 389–418.

Zafeiropoulou, A. M., Millard, D. E., Webber, C., & O'Hara, K. (2013). Unpicking the privacy paradox: Can structuration theory help to explain location-based privacy decisions? *Proceedings of the 5th Annual ACM Web Science Conference, WebSci'13*, *volume*, 463–472. https://doi.org/10.1145/2464464.2464503

Zimmer, J. C., Arsal, R. E., Al-Marzouq, M., & Grover, V. (2010). Investigating online information disclosure: Effects of information relevance, trust and risk. *Information and Management*, *47*(2), 115–123. https://doi.org/10.1016/j.im.2009.12.003

Zou, H. M., Sun, H., & Fang, Y. (2015). Understanding Post-Adoption Regret from the Perspectives of Herding and Mindfulness. *Thirty Sixth International Conference for Information Systems*, 1–19.

Figure 1. Protection Motivation Theory

Source: Adapted from Floyd, Prentice-Dunn and Rogers (2000)

Figure 2. Proposed theoretical model

Figure 3. Willingness to share different types of data

Figure 4. Structural model presenting path coefficients

Table 1. Demographic information of the participants in the survey

	Value	Percentage (%)
Gender	Male	47.2
	Female	52.4
	Other	0.4
Age	<26	5.0
	26-35	24.0
	36-45	12.0
	46-55	17.0
	56-65	22.0
	>65	20.0
Education	Less than High School	3.0
	High School	39.0
	BSc	35.0
	MSc	14.0
	PhD	4.0
	Other	5.0
Work status	Self Employed	11.5
	Private Sector	37.1
	Government	11.7
	Retired	25.3
	Unemployed	4.8
	Other	9.6
Online Shopping frequency	Daily	9.8
	Several times a week	21.0
	Several times a month	41.3
	Roughly once a month	23.5
	Almost Never	4.4

Table 2. Descriptive Statistics, Construct Reliability, Convergent and Discriminant Validity

Mean	Std. Dev	AVE	CR	Cronbach a'	Construct	(1)	(2)	(3)
3.69	0.615	0.625	0.948	0.924	(1) Privacy Concerns	**0.791**		
4.18	0.832	0.701	0.875	0.905	(2) Mindfulness	-0.199	**0.837**	
2.56	0.755	0.582	0.930	0.925	(3) Willingness to share data	-0.081	-0.148	**0.763**

Note: the diagonal elements (bold) indicate the square root of variance for each construct

Table 3. Goodness-of-fit assessments for the measurement and structural model

Goodness of Fit Measures	χ^2	χ^2/df	**CFI**	**RMSEA**	**GFI**	**AGFI**
CFA model	1291.935	5.273	0.926	0.079	0.850	0.816
SEM Model	1415.945	4.883	0.922	0.075	0.850	0.819

Table 4. Structural model results

Hypothesis	**Path coefficients**	**Result**
H1: Mindfulness → Privacy Concerns (-)	-0.216**	Supported
H2: Privacy Concerns → Willingness to share information (-)	-0.077*	Supported
Gender → Willingness to share information (-)	-0.089*	Supported
Age → Willingness to share information (-)	-0.117*	Supported
Education → Willingness to share information (-)	-0.072NS	Not Supported
Age → Privacy Concerns (+)	0.097*	Supported
Gender → Privacy Concerns (-)	-0.010NS	Not Supported
Education → Privacy Concerns (+)	0.032NS	Not Supported

Note: Significant at ** $p< 0.001$, * $p<0.05$, NS non-significant

Table 5. Mediation analysis

Relationship	**Direct effect**	**Indirect effect**	**Total effect**
Mindfulness-> Privacy Concerns -> Willingness to share	b=-0.174***	b=0.021**	b=-0.153***

Note: Significant at ** p< 0.001, * p<0.05, NS non-significant

Appendix A

Exploratory Factor Analysis (EFA)

The construct of willingness to share information with online companies was self-developed for the purposes of the present study. As a result, EFA with Maximum Likelihood and Promax rotation was implemented producing the results presented in Table A1. Three items of the construct were not retained due to very low loadings (less than 0.05) while the rest of them showed adequate factor loadings. Results are presented in Table A1.

Table A1. Exploratory Factor Analysis for Willingness to Share Information

Item	Loading	Eigenvalue	Percentage of Variance Explained	Cumulative percentage of variance explained
WL1	0.869	9.101	39.572	39.572
WL2	0.757	4.198	18.250	57.822
WL3	0.755	1.884	8.191	66.013
WL4	0.855	1.127	4.901	70.914
WL5	0.651	0.911	3.963	74.877
WL7	0.731	0.569	2.476	80.647
WL8	0.739	0.519	2.256	82.903
WL9	0.578	0.433	1.885	84.787
WL11	0.856	0.394	1.713	88.347
WL12	0.690	0.353	1.534	89.881
WL13	0.937	0.330	1.435	91.316
WL14	0.933	0.289	1.257	92.573
WL15	0.940	0.270	1.174	93.747
WL16	0.994	0.265	1.152	94.899
WL17	0.530	0.249	1.084	95.983
WL18	0.800	0.242	1.054	97.037
WL20	0.688	0.194	0.843	98.786
WL21	0.637	0.123	0.533	99.320
WL22	0.826	0.089	0.388	99.707
WL23	0.748	0.067	0.293	100.000

Common Method Bias

Table A2. Correlation estimates

Construct	**Estimate**
Privacy Concerns <-> Mindfulness	-0.199
Willingness to Share <-> Mindfulness	-0.148
Privacy Concerns <-> Willingness to Share	-0.081

Table A3. Multicollinearity estimates for all independent variables

Construct	**VIF**
Privacy Concerns	1.00
Mindfulness	1.00

Confirmatory Factor Analysis (CFA)

Table A4. Measurement and internal validity (CFA)

Privacy Concerns	**Loading**	**Mean**	**Std**
TOPC1	0.799	3.410	0.950
TOPC2	0.753	3.269	0.996
TOPC3	0.795	3.298	0.971
TOPC4	0.720	3.366	0.965
TOPC5	0.712	3.444	0.965
TOPC6	0.831	3.091	0.980
TOPC7	0.724	3.438	0.987
TOPC8	0.843	3.334	1.009
TOPC9	0.855	3.239	0.999
TOPC10	0.770	3.238	1.061
TOPC11	0.877	3.364	1.002
Mindfulness	**Loading**	**Mean**	**Std**
M1	0.605	4.295	1.166
M2	0.618	4.636	1.218
M3	0.698	4.553	1.235
M4	0.570	3.972	1.340
M7	0.762	4.197	1.253
M8	0.799	4.342	1.221
M9	0.567	4.104	1.215
M10	0.675	3.942	1.208
M11	0.547	3.509	1.228
M12	0.626	4.542	1.371
M13	0.619	3.812	1.348
M14	0.827	4.093	1.224

M15	0.583	4.774	1.335
Willingness to Share	**Loading**	**Mean**	**Std**
WL12	0.526	2.092	1.253
WL13	0.937	1.689	1.117
WL14	0.953	1.701	1.108
WL15	0.937	1.691	1.103
WL16	0.965	1.673	1.093
WL17	0.690	1.857	1.160
WL20	0.524	2.394	1.224
WL21	0.680	1.787	1.126
WL22	0.646	2.004	1.202
WL23	0.567	2.142	1.263

Appendix B

Mindfulness (MAAS) (Brown and Ryan, 2003)

M1 – **"***I could be experiencing some emotion and not be conscious of it until sometime later."*
M2 – "*I break or spill things because of carelessness, not paying attention, or thinking of something else."*
M3 – *"I find it difficult to stay focused on what's happening in the present."*
M4 – "*I tend to walk quickly to get where I'm going without paying attention to what I experience along the way."*
M5 – "*I tend not to notice feelings of physical tension or discomfort until they really grab my attention."*
M6 – " *I forget a person's name almost as soon as I've been told it for the first time."*
M7 – "*It seems I am "running on automatic," without much awareness of what I'm doing."*
M8 – " *I rush through activities without being really attentive to them."*
M9 – "*I get so focused on the goal I want to achieve that I lose touch with what I'm doing right now to get there."*
M10 – *"I do jobs or tasks automatically, without being aware of what I'm doing."*
M11 – "*I find myself listening to someone with one ear, doing something else at the same time."*
M12 – *"I drive places on 'automatic pilot' and then wonder why I went there."*
M13 – *"I find myself preoccupied with the future or the past."*
M14 – *"I find myself doing things without paying attention."*
M15 – *"I snack without being aware that I'm eating."*

Online Privacy Concerns (TOPC) (Smith, Milberg, & Burke, 1996; Xu, Dinev, Smith, & Hart, 2011;Wozniak, Schaffner, Stanoevska-Slabeva, & Lenz-Kesekamp, 2018)

TOPC1 – "*I am concerned that the information I submit to online travel companies could be misused."*
TOPC2 – "*I am concerned that others can find private information about me from online travel companies."*
TOPC3 – "*I am concerned about providing personal information to online travel companies, because it could be used in a way I did not foresee."*
TOPC4 – "*I don't feel comfortable when I do not have control over personal data I disclose to online travel companies."*
TOPC5 – "*I don't feel comfortable when I do not have control or autonomy over decisions about how my personal information is collected, used, and possibly shared by online travel companies."*
TOPC6 – "*It usually bothers me when online travel companies ask me for personal information."*
TOPC7 – "*When online travel companies ask me for personal information, I sometimes think twice before providing it."*
TOPC8 – "*It bothers me to give personal information to so many online travel companies."*
TOPC9 – "*I'm concerned that online travel companies are collecting too much information about me."*
TOPC10 – "*I don't feel comfortable to share information about my current location with online travel companies."*
TOPC11 – "*I am concerned with the security of sensitive information when I use online travel companies."*
TOPC12 – "*When people give personal information to an online travel company for some reason, the online company should never use the information for any other reason."*
TOPC13 – "*Online travel companies should never sell the personal information in their computer databases to companies."*
TOPC14 – "*Online travel companies should never share personal information with other companies unless it has been authorized by the individuals who provided the information."*

TOPC15 – "*Online travel companies should devote more time and effort to preventing unauthorized access to personal information."*
TOPC16 – "*Computer databases that contain personal information should be protected from unauthorized access no matter how much it costs."*
TOPC17 – "*Online travel companies should take more steps to make sure that unauthorized people cannot access personal information in their computers."*

Willingness to Share Information *(*self-developed)
"How willing are you to share the following information with online travel companies?"

WL1: Name
WL2: Date of birth
WL3: Home address
WL4: Email address
WL5: Phone number
WL6: Profession
WL7: Education
WL8: Credit card information
WL9: Bank account information
WL10: Contacts in address book
WL11: Passport number
WL12: Driver license number
WL13: Fingerprint
WL14: Voice sample
WL15: Face scan/image
WL16: Iris/retina pattern
WL17: Social media profile data
WL18: Hobbies/personal interests
WL19: Personal preferences (room selection in a hotel, dietary requirements)
WL20: Real time position
WL21: Smartphone search history (cookies)
WL22: Activity sensor data (body movements, number of steps, floors etc)
WL23: Specific expenses in places travelled and services purchased