European Journal of Marketing

Data vulnerability: does privacy protection behaviour improve digital well-being?

Sara Quach
Department of Marketing, Griffith Business School, Griffith University, Nathan, Australia

Simon Dang
Department of Business Administration, Economics Faculty, Nong Lam University, Ho Chi Minh, Vietnam, and Department of Marketing, Griffith Business School, Griffith University, Nathan, Australia

Park Thaichon
Department of Marketing, University of Southern Queensland, Toowoomba, Australia

Dung Le
College of Business and Management, VinUniversity, Hanoi, Vietnam, and

Truc H.H. Le
Department of Tourism, Sport and Hotel Management, Griffith Business School, Griffith University, Nathan, Australia

Received 31 December 2022
Revised 20 February 2024
8 September 2024
26 January 2025
Accepted 2 July 2025

Abstract

Purpose – This study aims to determine the relationship among data vulnerability, privacy concerns, privacy protection behaviours and online subjective well-being, with a focus on the moderating role of customers' emotional exhaustion.

Design/methodology/approach – Data was collected from 706 participants in the USA using an online survey. Structural equation modelling was used to analyse the data.

Findings – Data vulnerability increases privacy concerns, which in turn influence privacy protection behaviours. There was a positive relationship between online well-being and proactive protection behaviour, whereas reactive responses did not have a significant impact on online well-being. Emotional exhaustion augmented the impact of data vulnerability on privacy concerns and the effect of privacy concerns on reactive protection behaviours. The negative impact of vulnerability on consumers' well-being was weakened in the presence of high emotional exhaustion.

Research limitations/implications – Privacy concerns play a central role in the relationship between vulnerability, behavioural responses (i.e. protection behaviours) and consumers' well-being. However, effective measures to improve customer privacy need to consider the presence of emotional exhaustion.

Funding: This research was funded by Vingroup Innovation Foundation (VINIF) under project code VINIF.2022.DA00087.

European Journal of Marketing
Vol. 59 No. 13, 2025
pp. 207-239
Emerald Publishing Limited
0309-0566
DOI 10.1108/EJM-12-2022-0953

Practical implications – Privacy concerns play a central role in the relationship between vulnerability, behavioural responses (i.e. protection behaviours) and consumers' well-being. Firms' initiatives such as privacy by design and rights management are highly recommended because they prevent privacy-pervasive events and ensure minimal malicious and accidental breaches, thereby reducing customer vulnerability.

Originality/value – This study uniquely explores the role of emotional exhaustion in shaping customers' coping mechanisms for privacy issues, which, in turn, affects their subjective online well-being. It also introduces and validates the scales for measuring both proactive and reactive privacy protection behaviours.

Keywords Well-being, Privacy, Emotional exhaustion, Privacy concerns, Data vulnerability
Online well-being, Privacy protection behaviour

Paper type Research paper

Introduction

Advanced information and communication technologies have empowered firms to create more value for their customers (Kramer and Krafft, 2023; Sashi, 2021). Companies take advantage of the huge amount of data collected from Internet users to create sophisticated profiles of customers and target them using personalised offerings (Quach *et al.*, 2022). However, such actions also intensify customers' data vulnerability, which refers to the extent to which one is susceptible to harm on account of unauthorised usage of their personal information (Martin *et al.*, 2017). Data harnessing and monetising are becoming more common, without consumers' awareness and control (Quach *et al.*, 2022). This is particularly alarming when data breaches have become more common, putting customers' personal information at risk (Janakiraman *et al.*, 2018; Tunggal, 2022). These feelings can make customers become more anxious about their privacy and react negatively during their interactions with firms (Palmatier and Martin, 2019). Notwithstanding, there is limited understanding of how customers cope with the perception of data vulnerability. Our literature review identified only two studies directly addressing this issue. One study examines how customers cope with vulnerability perceptions by developing negative emotions within social networking sites (Cho *et al.*, 2010), while the other investigates the role of privacy concerns in mobile app usage (Chennamaneni and Gupta, 2023). Although the process of threat appraisal (i.e. perceived vulnerability) that triggers privacy concerns and leads to privacy protection behaviours has been identified (Chennamaneni and Gupta, 2023), ambiguity persists regarding how these behaviours impact users' online well-being and the role of other psychological factors during this process. To address this gap, we adopt the antecedents–privacy concerns–outcomes (APCO) model (Buck *et al.*, 2022) to explore further the effect of customer data vulnerability as an antecedent to customer privacy and its subsequent behavioural and psychological outcomes.

Being more suspicious about how their data is obtained and shared (Bright *et al.*, 2021), online users are increasingly worried that their digital footprints are recorded and used without their consent or knowledge (Bandara *et al.*, 2021). As privacy becomes a prevalent issue, it is imperative to understand its impact on customers. According to the meta-analytic review of Okazaki *et al.* (2020), although much research has been done on the linkage between privacy concerns and outcomes, most studies focus on the evaluative outcomes such as product, service and firm evaluations, trust and perceived risks as well as behavioural outcomes such as disclosure, purchase, use, the continuance of usage and privacy protection. Little attention has been paid to psychological outcomes such as customer well-being (Kwak *et al.*, 2021). Discussion about the impact of privacy issues needs to be extended to embrace the evolving digital environment, which has become increasingly more turbulent with a growing number of data breaches and data misuse incidents and an increase in the levels of stress and negative emotions (Labrecque *et al.*, 2021). Because these damaging feelings are

signals of degradation of life satisfaction, research needs to investigate consumers' subjective online well-being as an outcome of privacy concerns and behaviour.

Subjective well-being generally refers to individuals' cognitive and affective assessment of their own lives (Azizan and Mahmud, 2018), and online subjective well-being is a specific variant that focuses on emotional experiences in the digital world, such as satisfaction, happiness and both negative and positive reactions (Verduyn *et al.*, 2017). The seminal work of Schwartz (1968) underlines privacy's critical role in societal processes and individual well-being, highlighting its importance in protecting the human psyche. Furthermore, Palmatier and Martin (2019) argue that privacy is vital not just for self-protection and preservation benefits that enact social functioning, but also for psychological well-being. In today's digital age, where privacy concerns are increasingly significant, it is crucial to understand how privacy impacts consumers' psychological states online. Exploring online subjective well-being offers valuable insights into these effects and informs the development of effective privacy protection strategies. Building on the APCO model, which identifies behavioural reactions (e.g. privacy protection behaviours) as outcomes of privacy concerns, we propose that these actions also influence subjective online well-being as a consequence, aligning with the situation–organism–behaviour–consequence (SOBC) paradigm (Davis and Luthans, 1980). This study goes beyond previous research that treats privacy protection behaviour as the ultimate outcome (e.g. Bandara *et al.*, 2021; Lwin *et al.*, 2007) by examining the distinct effects of reactive and proactive behavioural responses on customer well-being.

Most research examines subjective online well-being from the use of social networking sites (SNSs) (Table 1), including active/passive use (Verduyn *et al.*, 2017), social capital and social presence (Erfani and Abedin, 2018). Webster *et al.* (2021) confirm the positive influence of offline social networks on young consumers' mood, self-esteem and loneliness, whereas there is a negative influence on adolescents' mood, self-esteem, life satisfaction, body image and overall subjective well-being because of high investment, passive use, negative feedback and spurning from social media. However, our review reveals a gap in understanding how data vulnerability and privacy responses affect customers' subjective online well-being. On the other hand, high privacy demand and limited cognitive resources might result in burnout and anxiety in consumers, increasing their emotional exhaustion (Agozie and Kaya, 2021). Fatigued individuals may deviate from typical responses as their capacity to process information diminishes, leading to low-effort processing or hasty judgement, aspects not accounted for in the APCO model (Dinev *et al.*, 2015). Lyu *et al.* (2024) highlighted the role of privacy fatigue, an organism mechanism, to explain how privacy invasion leads to privacy behaviours (i.e. protection disengagement) in using contactless digital services. Similarly, to explain how users cope with privacy risks from using smart speakers, Park *et al.* (2021) elucidate users' emotional reactions (i.e. organism mechanism) to privacy threats as stimulus. These studies support the notion that the SOBC paradigm allows for the integration of additional determinants, offering flexibility in advancing the APCO model by better explaining the bounded rationalities within its existing relationships. Therefore, we proposed that privacy emotional exhaustion can influence the effect of data vulnerability and privacy concerns on their subsequent outcomes, including protection behaviour and online well-being. This study, thus, seeks to address the following overall research question: "What mechanism underlies the impact of data vulnerability on consumers' privacy protection behaviour and online subjective well-being?" To address this inquiry, the paper has two primary objectives:

Table 1. Selected empirical research on privacy-related constructs and subjective (online) well-being

Antecedents	Well-being outcome	Study type	Data collection	Sample (size)	Country	Context	Methodology	Main findings*	References
• Relatedness needs satisfaction (+) • Interaction privacy control $^{+}$ • Self-disclosure $^{+}$	Life satisfaction	Cross-sectional	Online survey	General consumers (2,076)	South Korea	SNSs	EFA/CFA/SEM	Interaction privacy controls positively influence self-disclosure, and both enhance the satisfaction of relationship needs, which, in turn, boosts consumers' subjective well-being in the social network context	Chae *et al.* (2022)
• Information collection concerns (−) • Risk beliefs (−) • Trust beliefs (+) • Experience sharing frequency (+) (moderator)	Happiness	Cross-sectional	Online survey	General consumers (649)	France	SNSs	CFA/percentile and 5,000 bootstrap samples	Building on both social exchange and construal level theories, the study confirmed the most pivotal role of happiness with the internet on willingness to disclose information outperforming privacy-related constructs (i.e. trust and risk beliefs). Information collection concerns negatively affect happiness, whereas trust beliefs and experience-sharing frequency were found to positively enhance happiness with the internet. Also, the more users share their experiences on the internet, their privacy concerns (i.e. information collection concerns) are enhanced	Cloarec *et al.* (2022)

(*continued*)

Table 1. Continued

Antecedents	Well-being outcome	Study type	Data collection	Sample (size)	Country	Context	Methodology	Main findings*	References
• Stressful events (−) • Perceived social support (+) • Enacted social support (+) • Self-disclosure (ns)	Life satisfaction and depression	Cross-sectional	Paper-based survey	Students (560)	Hong Kong	SNSs	Zero-order correlations/ principal component analysis/ hierarchical regression analysis	On the one hand, the strongest predictor of depression was stressful life events. All stressors (i.e. academic, interpersonal and environmental) were positively related to depression. Perceived social support was marginal to reduce depression. High privacy demands and limited cognitive resources can contribute to consumer burnout and anxiety, thereby increasing emotional exhaustion (Agozie and Kaya, 2021). Although self-disclosure on facebook had no influence on depression and life satisfaction, it serves to moderate the relationship between stressful life events and mental health	Zhang (2017)
• Communicative use (+) • Friending (ns) • Self-disclosure (+) • Bonding social capital (+) • Bridging social capital (+)	Psychological well-being	Cross-sectional	Online survey	General consumers (813)	Hong Kong	SNSs	Hierarchical regression analysis	Findings illustrated a positive relationship between self-disclosure and communicative use and psychological well-being but not friending. Not only bonding and bridging social capital are critical mediators between mentioned constructs and well-being, but their direct impact on well-being also suggests greater life satisfaction can be promoted through interconnecting with people who share their values and beliefs (i.e. bonding) as well as	Chen and Li (2017)

(*continued*)

Table 1. Continued

Antecedents	Well-being outcome	Study type	Data collection	Sample (size)	Country	Context	Methodology	Main findings*	References
								with people who are different from them (i.e. bridging)	
• Authenticity (+)	Positive affect, negative affect and life satisfaction	Cross-sectional	Online survey	General consumers (374)	Germany	SNSs	Longitudinal analysis	In the SNSs environment, online authenticity is nurtured and given a forum for self-presentation; thus, its positive effects on psychological well-being are beneficial to users. However, authentic online behaviour is in accordance with users who already have a high level of well-being and can easily engage in positive authenticity. In contrast, the lower levels of well-being counterparts witness fewer benefits from expressing their authentic negative feelings and experiences, which is against the positive norms in the SNSs environment	Reinecke and Trepte (2014)

Note(s): SNSs: social networking sites; *only main findings related to subjective well-being are reported. Not direct antecedent. A preliminary search was conducted on Google Scholar using potential keywords such as "privacy", "subjective well-being" and "data vulnerability". After analysing the first 50 records, we refined the keywords to [subjective well-being AND ("privacy" OR "data vulnerability")] and used these to extract data from the two largest databases: Scopus and Web of Science. We included only empirical studies written in English that had subjective well-being as the outcome variable and involved privacy issues or protection behaviours. Review papers, editorials and books were excluded, as well as empirical studies that included subjective well-being outcomes without addressing privacy variables or actions. This process resulted in 30 relevant papers, of which five met the eligibility criteria and are included in the review
Source(s): Authors' own work

(1) to investigate data vulnerability as a driver of privacy concerns, protection responses (both proactive and reactive behaviours) and the ramifications on online subjective well-being; and

(2) to determine the moderating role of customers' emotional exhaustion in these relationships.

The study provides an important contribution to the current body of knowledge related to online subjective well-being and consumers' privacy. First, by integrating the APCO and SOBC paradigms, we extend previous research, which predominantly focuses on evaluative and behavioural outcomes of privacy concerns, by including online subjective well-being as a key consequence (Okazaki *et al.*, 2020). This enriches the conceptualisation of privacy as the ability to manage privacy threats by taking protection actions in response to perceived vulnerability to achieve online well-being (Palmatier and Martin 2019).

Second, our study provides evidence for the distinct effects of proactive and reactive protection behaviours within the APCO model, rather than solely examining general protection behaviours as seen in previous studies (e.g. Soomro and Hussain, 2019; Yang, 2013) or focusing predominantly on one type of response (e.g. van Ooijen *et al.*, 2022; Wisniewski *et al.*, 2015; Wottrich *et al.*, 2019). Quach *et al.* (2022) emphasised the importance of considering both proactive and reactive protection behaviours, as they represent distinct approaches to addressing privacy concerns in the digital landscape. Reactive protection behaviour involves responding to immediate threats or following explicit advice, while proactive protection behaviour involves preemptively addressing privacy threats and taking measures to prevent privacy risks from materialising. Although both types of protection behaviours aim to preserve consumers' privacy, they may have disparate effects on consumers' well-being because of differences in the level of social interaction required and the amount of effort involved. By acknowledging these differences, our study underscores the need for a nuanced approach when investigating consumers' privacy protection behaviour and subjective online well-being.

Finally, this study highlights the moderating role of emotional exhaustion, answering the call of Dinev *et al.* (2015). Going beyond recent studies (Augustin *et al.*, 2022; Choi *et al.*, 2018; Pomfret *et al.*, 2020), which suggest that fatigue decreases coping measures while increasing non-protective behaviours, we shed light on the boundary condition of emotional exhaustion in relationships between vulnerability, privacy concerns, two types of privacy protection behaviours and online subjective well-being. The paper provides important implications to marketers and customers about privacy protection. The following sections of the paper provide a review of the theoretical underpinnings of the study, research methods and the findings of the study. The paper concludes with a discussion of the results, research implications, limitations and future research directions.

Literature review

The antecedent–privacy concern–outcomes model

Previous research has proposed privacy concerns as a proxy for measuring privacy (Buck *et al.*, 2022). Following an interdisciplinary review of 320 privacy articles and 128 books and book sections, Smith *et al.* (2011) proposed the model, namely, the APCO model (antecedents → privacy concerns → outcomes), which has been the cornerstone for information privacy research. The APCO model rests on the assumption that consumers' deliberation from external stimuli drives their privacy-related responses and behaviours (Buck *et al.*, 2022). However, this rational premise that people operate on logical decisions has been challenged by privacy experts (Buck *et al.*, 2022; Palmatier and Martin, 2019), with

the privacy paradox highlighting inconsistent behaviours in the literature (Choi *et al.*, 2018; Dienlin and Trepte, 2015; Kokolakis, 2017; Norberg *et al.*, 2007). Indeed, when people suffer emotional distress or cognitive strain, their diminished cognitive processing capacity drives them to make effortless decisions such as self-disclosure and give up their personal information to swiftly reach a "fatigue" decision (Acquisti and Grossklags, 2005; Acquisti *et al.*, 2013; Shao *et al.*, 2022). As such, the fatigue concept has received attention from privacy scholars as a solution to explain the privacy paradox. Additionally, Palmatier and Martin (2019) placed more emphasis on the concept of vulnerability, because consumers lack an understanding of data privacy (Martin *et al.*, 2017). The rationality, thus, fits squarely in the APCO as an antecedent to inform heightened privacy concerns.

Furthermore, the outcome of the APCO model is behavioural reactions to privacy concerns but not the consequence of such reactions. According to the SOBC paradigm (Davis and Luthans, 1980), the environmental stimuli (S) prompt an individual organism (O) or mechanism, leading to behavioural responses (B), which subsequently affect covert or overt consequences (C). The paradigm integrates stimulus, internal processing and behaviour with the consequences, highlighting a feedback loop where outcomes, in turn, influence future stimuli, organism states and behaviours. The SOBC has been successfully used to explain related interaction contexts such as social media overload (Whelan *et al.*, 2020). Unlike the stimulus–organism–response paradigms, which typically focus on individual responses to specific situational stimuli, the SOBC paradigm expands its scope to encompass the broader environmental context. Specifically, as data vulnerability extends beyond isolated incidents of data loss or breaches, encompassing the pervasive risk inherent in the digital environment (Palmatier and Martin, 2019), it serves as a continuous backdrop shaping individuals' perceptions, emotions and cognitive assessments. This influence extends across various contexts, not just in response to specific events. Within the framework of the SOBC paradigm, engaging in privacy protection behaviours carries consequences for subjective well-being (Lombardi and Ciceri, 2016), emphasising an outcome that surpasses the confines of individual incidents. The emphasis on the broader environment within the SOBC paradigm allows for a deeper understanding of the mechanisms guiding individuals' responses to data vulnerability. Moreover, it underscores the significance of the mechanism shaping behavioural reactions to privacy concerns and the subsequent outcomes, highlighting that these effects are not solely confined to specific situations but have enduring implications across various contexts and over time. In that vein, SOBC improves APCO by considering the organism factor (i.e. emotional exhaustion) as a boundary condition and the consequence (i.e. subjective well-being) to extend the privacy coping process and outcomes (i.e. protection behaviours). Therefore, we propose that subjective online well-being can be a psychological outcome of privacy protection behaviours, and emotional exhaustion can explain the boundary condition for such antecedents–privacy concerns–behavioural reactions association in APCO. As such, the conceptual framework proposed in this study is based on an extended APCO model, incorporating the consequence (i.e. subjective well-being) of privacy reaction outcomes (i.e. protection behaviours) and the organism mechanism (i.e. emotional exhaustion).

Data vulnerability and privacy concerns. Unified from the famous conceptualisations of Westin and Altman, the control-centered definition of general privacy is defined as "Privacy, as a whole or in part, represents the control of transactions between the person(s) and other(s), the ultimate aim of which is to enhance autonomy and/or to minimise vulnerability" (Margulis, 1977, p. 10). Although those works existed way before the debut of digital privacy concerns, experts agree that privacy functions in society as a pivotal human necessity with corresponding benefits (Palmatier and Martin, 2019; Quach *et al.*, 2022). Nested in this

cognate-based definition of privacy is the linkage between privacy and the vulnerability concept, which emerges as a critical issue in the digital age. Indeed, data vulnerability is defined as users' susceptibility perception of falling victim to the exploitation and misuse of unauthorised personal data (Chou and Chou, 2021; Martin *et al.*, 2017).

In this context, the "data" notion specifically refers to identifiable information that relates to an individual, which can range from basic personal details to more sensitive types such as biometric and behavioural data. The concept of data vulnerability encapsulates individuals' overall subjective sentiment and perception of insecurity regarding their online presence and the digital footprints they generate. Thus, this research focuses on data vulnerability as individuals' perceptions of their insecurity, not the actual vulnerability stemming from unknown privacy intrusions. For example, consumers engaging in online shopping for the first time during the COVID-19 pandemic may exhibit heightened concerns regarding the privacy and security of their shopping data because of lack of experience, increased exposure to online risks, heightened awareness of cyber threats, the increased amount of personal data shared and trust issues with new platforms. As highlighted by Martin *et al.* (2017), there is an inverse relationship between the reliability of the environment and consumer vulnerability, implying that individuals feel less vulnerable when using a trusted and secure service. For instance, e-commerce platforms such as Amazon and Shopify, known for their robust security measures and customer service, including secure payment gateways and buyer protection policies, often foster a sense of safety among users. Similarly, users tend to feel secure when accessing major banks' websites or apps because of their trust in the institutions' reputation and visible security measures, such as encryption, secure login procedures and fraud alerts. In line with this, the connection between data vulnerability and privacy concerns has been well-conceptualised in mainstream privacy research. Also, privacy concern, a focal psychological construct in the field of marketing and consumer study (Pomfret *et al.*, 2020), constitutes the negative feeling towards the intrusions of an individual's rights and information (Dienlin and Trepte, 2015).

Consumers' privacy concerns are amplified in the presence of a sense of vulnerability to privacy invasion (Palmatier and Martin, 2019). In fact, in the digital era, highly sensitive and personal data (e.g. medical conditions, physical activity) from a multitude of sources (e.g. social media, geospatial, biometrics and web tracking technologies), in the era of digital 4.0, are subject to various types of monetisation (Quach *et al.*, 2022). Therefore, a feeling of data vulnerability can heighten privacy concerns. Besides, vulnerability hints at susceptibility to harm or being exploited by others, which limits one's ability to maximise their utility and well-being (Smith and Cooper-Martin, 1997). This explains how anxious consumers feel when their information is at stake from potential damage or feelings of violation rather than the actual incidence of data misuse or harm (Palmatier and Martin, 2019). As such, it is expected that the detrimental effect of data vulnerability with negative emotions (i.e. depression or anxiety) can deteriorate consumers' online subjective well-being, which refers to satisfaction with life overall (Azizan and Mahmud, 2018; Rahman, 2021; Voukelatou *et al.*, 2021). On the basis of the foregoing discussion, we hypothesise the following:

H1. Data vulnerability is positively related to privacy concerns.

H2. Data vulnerability is negatively related to online well-being.

Privacy responses. Privacy literature has documented two main types of privacy management strategies, namely, reactive and proactive responses (Quach *et al.*, 2022). While proactive protection is preventive measures (e.g. using privacy-enhancing technologies) conducted beforehand to avoid information leakage without involving interpersonal

relationships, reactive protection denotes actions in response to an occurred privacy incident and often involves reducing or changing social interaction to deal with privacy intrusions (e.g. untagging oneself from a social media post) (Chou and Chou, 2021). Past and recent privacy literature has pointed out the positive relationship between privacy concerns and privacy protection behaviour (Baruh *et al.*, 2017; Strycharz *et al.*, 2019; Wottrich *et al.*, 2019; Yang, 2013). In the Helsinki Privacy Experiment of household surveillance, a mixture of privacy-seeking behaviours was observed, both active privacy-seeking means (proactive), such as going to the café to discuss personal matters, and reactive means, such as avoiding nudity, sexual intercourse or alcohol/substance use in front of the camera (Oulasvirta *et al.*, 2012). As such, it is expected that privacy concerns can increase both reactive and proactive privacy protection behaviours. We proposed the following hypothesis:

H3. Privacy concerns are positively related to (a) reactive privacy protection behaviour and (b) proactive privacy protection behaviour.

Research into the psychological functions of privacy suggested that privacy can be considered as a boundary control process involving restricting and seeking interaction to attain a desirable amount of access to self or others (Pedersen, 1997). Lombardi and Ciceri (2016) argue that because of frequent privacy intrusions in digital space, privacy protection is a prerequisite for obtaining privacy and its quality of well-being. Furthermore, it is also worth noting that achieving the preferable amount of social interaction can be challenging, as too much interaction might lead to privacy invasion, and too little yields isolation or a sense of detachment (Pedersen, 1997). In this vein, proactive and reactive protection are distinctive regarding interaction with others or interpersonal conflicts. If proactive protection is analogous to personal management without involving social relationships (De Wolf, 2020), reactive protection requires users to take interpersonal resorts or tradeoffs (Chou and Chou, 2021) in the social capital building; for example, untagging themselves from a friend's social media post might be considered exasperated (Wisniewski *et al.*, 2015).

Thus, we argue that, although both protection behaviours aim to preserve consumers' privacy, they might have the opposite effect on consumers' well-being because of tradeoffs in the social interaction required and the level of effort. In other words, the increased reactive protection corresponds to an equivalent effort spent to deal with privacy problems that have already happened and often involve unfavourable changes in social interactions, thus might be jeopardising one's well-being. In contrast, proactive protection is deployed in advance to deter any potential issues arising, which, in turn, might enhance life satisfaction and lessen distress. Hence, we posit the following:

H4. Reactive privacy protection behaviour is negatively related to online well-being.

H5. Proactive privacy protection behaviour is positively related to online well-being.

The moderating role of privacy emotional exhaustion. Emerging from Mashlach's burnout framework, emotional exhaustion was defined as "a chronic state of emotional and physical depletion" (Cropanzano *et al.*, 2003, p. 160). Emotional exhaustion best captures the elemental meaning of burnout (Shirom, 1989) and constitutes a core component of the concept of fatigue drawn from burnout literature (Agozie and Kaya, 2021; Choi *et al.*, 2018; Tang *et al.*, 2021). Unlike privacy cynicism, which involves frustration, hopelessness and disillusionment because of unmet expectations, emotional exhaustion relates to a sense of tiredness arising from privacy demands (Choi *et al.*, 2018). Fatigued people are deviated from rational privacy choices because of reduced efficacy in processing apposite information (Acquisti *et al.*, 2013), which eventually results in the inefficient performance of tasks or

activities (Choi *et al.*, 2018). Because exhausted people are of a low level of hardiness (i.e. daily activity involvement, a sense of control and openness to change) under high workload and stress (Maslach *et al.*, 2001), and emotional exhaustion also signals emotional and physical depletion (Cropanzano *et al.*, 2003), it is plausible that among exhausted people who experience a heightened sense of helplessness, the effect of data vulnerability on privacy concern will be greater than those who remain energetic in terms of privacy. On the other hand, the impact of data vulnerability on well-being (*H2*) can be reduced in the presence of emotional exhaustion. Indeed, the Helsinki privacy experiment has offered useful evidence to prove that chronically privacy-intruded users tend to accept the situation to the point that their annoyance and anxiety fade away and begin to feel normal with the surveillance (Oulasvirta *et al.*, 2012). Therefore, we suggest the following hypotheses:

H6. Privacy emotional exhaustion moderates the effect of data vulnerability on privacy concerns, in which the positive effect of data vulnerability on privacy concerns will be stronger at a higher level of privacy emotional exhaustion.

H7. Privacy emotional exhaustion moderates the effect of data vulnerability on online well-being, in which the negative effect of data vulnerability on well-being will be weaker at a higher level of privacy emotional exhaustion.

The privacy paradox is a well-known phenomenon in which people are willing to share their personal information while manifesting a high degree of privacy concern (Norberg *et al.*, 2007; Pomfret *et al.*, 2020). In spite of great attention given to untangling this paradoxical outcome through multiple concepts such as the privacy calculus or the privacy cynicism (Augustin *et al.*, 2022), the underpinning mechanism and a mutually agreed cross-disciplinary explanation are far from being achieved (Baruh *et al.*, 2017; Kokolakis, 2017; Pomfret *et al.*, 2020). In light of the privacy calculus theory, the act of privacy information disclosure is an empowering exercise of control over the act itself (Dinev *et al.*, 2013), and purposeful cost–benefit tradeoffs were made before conducting privacy-related decisions; while some consumers find the benefits of privacy sharing outweigh its costs of consequences and make rational sharing decisions, others exercise a calculus refusing to trade their personal information for inequivalent benefits (Palmatier and Martin, 2019). Choi *et al.* (2018) reported that privacy fatigue weakens the negative relationship between privacy concerns and online non-protective behaviours (i.e. disclosure of personal information and disengagement coping). Intuitively, the same mentality can also be applied to privacy coping measures because those with fatigue would want to diminish decision-making effort (Levav *et al.*, 2010). We argue that reactive protection measures are actions that can be taken at a later stage only when privacy issues occur, whereas proactive measures refer to preventive treatments that need to be taken now to prevent later incidences. As protective measures demand more time and effort, and as individuals become more emotionally exhausted, the effect of privacy concerns will be stronger for reactive protection behaviour but weaker for proactive responses. Therefore, we hypothesise the following:

H8. Privacy emotional exhaustion moderates the effect of privacy concerns on privacy protection behaviour, which will amplify the effect of privacy concerns on reactive behaviour not on proactive behaviour.

The proposed conceptual framework, which extends the APCO model to include protection behaviours and subjective well-being as the consequences of privacy outcomes, is illustrated in Figure 1. We discussed the data collection process and provided details about the measurement scales for the constructs in the model in the following methodology section.

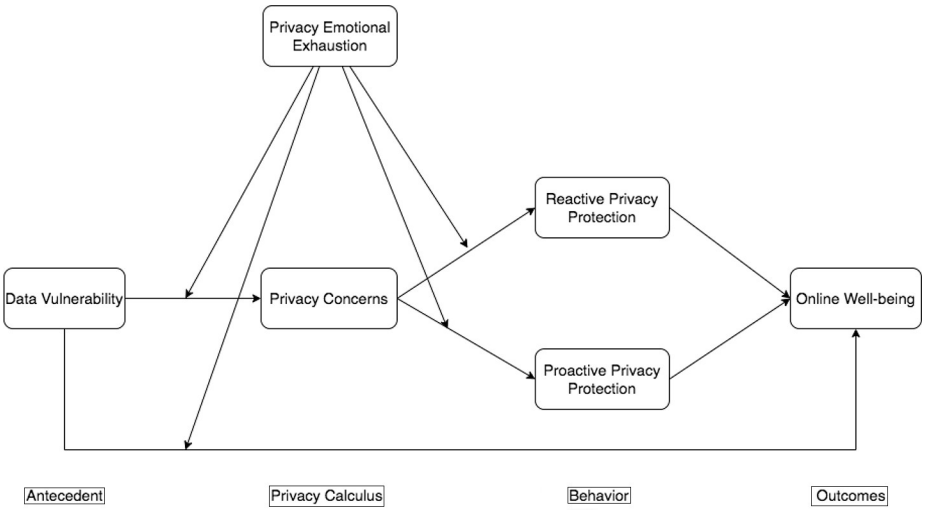

Figure 1. The proposed framework antecedents–privacy concerns–behaviour–outcomes (APBO) based on the enhanced APCO model (Dinev *et al.*, 2015) and SOBC (Davis and Luthans, 1980)
Source: Authors' own work

Methodology

Data collection

We recruited 706 participants on MTurk, which is an online platform that facilitates crowdsourcing by connecting requesters with a large pool of participants who can perform various tasks, including survey participation (Aguinis *et al.*, 2021). MTurk was selected for its efficiency in providing a diverse and substantial participant pool, crucial for statistical analysis (Goodman and Paolacci, 2017). The study aims to explore the relationships among data vulnerability, privacy concerns, privacy protection behaviours and online subjective well-being, while also examining the moderating role of emotional exhaustion. The choice to use an online survey for data collection is particularly fitting, given the digital nature of the research focus. Collecting data through an online platform not only ensures relevance but also provides access to a diverse sample of participants who are directly engaged with these issues in their daily lives.

While MTurk offers convenience, we acknowledge a primary concern is the quality and engagement of participants. MTurk workers may not always engage with the survey as attentively as a more carefully selected sample, potentially leading to variability in data quality. This variability could affect the reliability of findings. Therefore, we implemented several quality control measures, including strict screening criteria (only accepting respondents with a 95% approval rate who resided in the USA) and attention checks such as "It is important to pay attention to the survey. Please choose strongly disagree" to verify that respondents were paying attention and providing legitimate responses. These checks were designed to filter out any participants who might not have been fully engaged with the survey, ensuring the integrity of our data. We dropped 94 responses that were incomplete or failed the two attention checks. The final sample size was 706, including a range of respondents to account for various levels of digital engagement. This approach allowed us to capture a wider spectrum of experiences and perceptions, thereby providing a more

comprehensive understanding of the different levels of vulnerability among users of digital technologies. In the final sample, 44.5% of them were females. A total of 60.2% had a bachelor's degree and 22% had a postgraduate degree. 30.7% of the respondents were from 18 to 28 years old, 36.5% from 29 to 38 years old, 17.7% from 39 to 48 years old, 10.2% from 49 to 58 years old and 4.8% from 59 years old or older. In terms of education, 12.7% of the respondents picked high school as their highest qualification, 5.1% vocational education, 60.2% bachelor's degree and 22% postgraduate degree. In terms of income, 21.2% earned less than $35,000, 17.7% earned between $35,000 and $49,999, 26.2% between $50,000 and $74,999, 22.8% between $75,000 and $99,999, and 12.1% from $100,000.

Measures

Previously validated scales were adapted to measure the constructs in this study. Data vulnerability and privacy concerns were measured using the scales from Martin, Borah and Palmatier (2017), in which respondents were asked how they felt about the personal information that businesses had about them. Here, "data" refers to identifiable information about an individual, and "data vulnerability" encompasses the overall sentiment that consumers hold regarding their online experiences. Given the substantial digital footprint left by Internet users because of their reliance on digital technologies, this study specifically explores participants' reflections on their feelings about the personal information held by businesses. The data vulnerability measures focus on evaluating the extent to which individuals perceive themselves as insecure, vulnerable and susceptible to potential harm resulting from the disclosure of their personal data. The emotional exhaustion scale was taken from Choi *et al.* (2018), and online subjective well-being from Kaur *et al.* (2021). All constructs were measured using a seven-point Likert scale.

The items of the privacy protection behaviour were developed based on the typology of privacy protection by Quach *et al.* (2022) and interviews with five customers in a pilot study. Specifically, we conducted interviews with five consumer informants aged 27–41 years of age, all of whom were avid users of digital technologies. The primary goal of these interviews was to gain preliminary insights and refine the items used in our main study, rather than to generalise findings. Therefore, a sample size of five can be adequate for identifying common themes and insights (Guest, Namey, and Mitchell, 2013), particularly when the objective is to explore the overall behaviours and attitudes. The five informants interviewed were not restricted to a specific product but were selected based on their diverse experiences with digital technologies. They were from various countries, including China, Australia, Vietnam and Thailand, which helped provide a broader perspective on privacy behaviours and concerns. This diversity was intentional to capture a range of experiences and insights that could inform the development of our survey items. We identified our participants through our network within a research cluster. The interviews were carried out through either face-to-face interactions or via a video conference platform, with the sessions recorded and subsequently transcribed. Our interview protocol consisted of 18 questions that delved into topics such as digital technologies, data collection and utilisation and privacy protection behaviour. These questions were structured based on the conceptualisation of proactive and reactive behaviour outlined by Quach *et al.* (2022).

Our study explores the broader landscape of online experiences instead of focusing on a specific industry. This wide-ranging approach is driven by the recognition that heavy reliance on technology may contribute to a decline in mental well-being (Dienlin and Johannes, 2020). The primary objective of our pilot interviews was to refine the items in our study. To ensure the face and content validity of our measures, we engaged in iterative discussions with the interview participants. These discussions involved reviewing and refining our

measures based on their feedback to ensure that the items accurately captured key constructs, such as privacy protection behaviours and data vulnerability. Additionally, we used previously validated scales to measure data vulnerability and privacy concerns (Martin, Borah and Palmatier, 2017) as well as emotional exhaustion (Choi *et al.*, 2018). This approach, combined with the pilot interviews, helped confirm that our measures were both relevant and reliable for the broader study. Through iterative discussions and analysis, the five participants reached a consensus on the most common behaviours used to protect their data. This convergence among informants strengthened our confidence in the validity and representativeness of the insights gathered, affirming the adequacy of our chosen sample size. As the result of the pilot study, we excluded underperforming items, namely, "I use The Onion Router", "I use virtual private networks (VPNs)" and "I delete apps when being asked for information". This could be because of the limited popularity of third-party applications within the general population. Additionally, the act of deleting apps in response to information requests has become less prevalent, given the widespread practice of apps requiring information in today's digital landscape. Age, gender, education and income were included as control variables, as they might influence customer privacy behaviour and perception of well-being. Following Podsakoff *et al.* (2003), respondents were assured about the anonymity of the survey responses and informed that there were no right or wrong answers. This helped minimise common method bias (Bandara *et al.*, 2021). We report the validity and reliability of constructs in the below section.

Data analysis

Validity and reliability of constructs

Given that privacy protection behaviour was measured via scale items not previously validated in the literature, construct validity was conducted on the measurement items of the latent constructs using Exploratory Factor Analysis (EFA). Before performing EFA, the data were randomly split into halves. EFA was conducted in the first half, and confirmatory factor analysis (CFA) was conducted in the second half to determine whether the factor structures required any modification. During this process, items were inspected for poor factor loadings (i.e. < 0.50), significant cross-loadings (i.e. > 0.40) (Schertzer *et al.*, 2008) and poor-performing items ("I turn to other non-digital alternatives such as face-to-face communication and traditional media", and "I minimize disclosing my information in public platforms such as in social media posts and comments") were dropped from further analyses. As digital behaviours evolve, certain practices may become less common or less relevant, affecting their effectiveness. The remaining data produced satisfactory factor loadings (i.e. ranging from 0.586 to 0.905) for each of the constructs (Fornell and Larcker, 1981). All constructs were unidimensional. CFA was conducted using IBM AMOS 28, and the results are provided in Table 2.

According to Table 2, construct reliabilities range from 0.818 to 0.911 and the factor loadings range from 0.672 to 0.915. Composite reliabilities (CRs), average variance extracted (AVEs) and correlations are provided in Table 3. The fit statistics for the accompanying CFA were satisfactory: $\chi^2(194) = 490.002$ ($p < 0.01$), standardized root mean square residual (SRMR) = 0.031, root mean square error of approximation (RMSEA) = 0.047, comparative fit index (CFI) = 0.969, NFI = 0.950 and goodness-of-fit index (GFI) = 0.939. All of the CRs were greater than the 0.70 threshold (Nunnally and Bernstein, 1994), and AVEs were higher than the recommended 0.50 (Hair *et al.*, 2016), demonstrating convergent validity. The correlations and descriptive statistics of the constructs are provided in Table 2. Moreover, squared correlation coefficients between each

Table 2. Confirmatory factor analysis results

Scale items	Standardised coefficients	AVE	CR
Data vulnerability		0.836	0.911
(1) Insecure	0.841		
(2) Vulnerable	0.915		
(3) Susceptible	0.914		
Privacy concerns		0.620	0.830
(1) How concerned are you that your personal data may be used for purposes other than the reason you provided the information for?	0.764		
(2) How concerned are you about the fact that this business might know/track your digital behaviour?	0.842		
(3) How concerned are you that other parties will be able to access your information at this business?	0.753		
Privacy emotional exhaustion		0.708	0.879
(1) I am tired of online privacy issues	0.889		
(2) It is tiresome for me to care about online privacy	0.749		
(3) I am tired of managing privacy in an online environment	0.879		
Reactive privacy protection behaviour		0.686	0.897
(1) I refuse to provide information when asked by an online business	0.793		
(2) I delete or edit past posts to protect my information	0.836		
(3) I contact the company to remove personal details	0.838		
(4) I remove tags of my names in social media posts	0.844		
Proactive privacy protection behaviour		0.529	0.818
(1) I check server security (i.e. https) when visiting an online website	0.688		
(2) I change cookie settings on websites that I visit	0.772		
(3) I use privacy-enhancing technologies such as pop-up window blockers and firewalls	0.734		
(4) I use internet security programs	0.713		
Digital well-being		0.597	0.881
(1) The conditions of my online experiences are excellent	0.825		
(2) I am satisfied with my online experiences	0.780		
(3) So far, I have obtained important things I want from online experiences	0.672		
(4) At present, I am completely satisfied with my online experiences	0.794		
(5) I feel happy about the personal aspects (achievements, health, etc.) of my online experiences	0.785		

Source(s): Authors' own work

Table 3. Correlations and descriptive statistics

	Mean	SD	Vulnerability	Privacy concerns	Reactive protection behaviour	Proactive protection behaviour	Online well-being	Privacy emotional exhaustion
Vulnerability	4.534	1.64373	*0.914*					
Privacy concerns	5.2554	1.23314	0.507	*0.787*				
Reactive protection behaviour	4.4143	1.67096	0.678	0.596	*0.828*			
Proactive protection behaviour	4.9267	1.34033	0.468	0.673	0.725	*0.727*		
Online well-being	5.383	0.99254	0.173	0.335	0.309	0.497	*0.772*	
Privacy emotional exhaustion	5.0619	1.39099	0.601	0.401	0.647	0.422	0.309	*0.841*

Note(s): The diagonal elements are the squared AVEs (italics). The lower left triangle elements are correlations among constructs. All correlations were significant at $p < 0.01$
Source(s): Authors' own work

pair of constructs in the model were below the corresponding AVEs (Table 3), confirming discriminant validity (Fornell and Larcker, 1981).

Age and gender differences

We have conducted an independent sample *t*-test to test the difference between males and females on emotional exhaustion. The results show no difference between males and females (M_{female} = 5.037, SD_{female} = 1.319, M_{male} = 5.092, SD_{male} = 1.477, t(704) =0.521, p = 0.602). In addition, a regression analysis suggested that age did not have a significant effect on emotional exhaustion (B = 0.010, SE = 0.046, t = 0.219, p = 0.827).

In terms of privacy concerns, the results show no difference between males and females (M_{female} = 5.230, SD_{female} = 1.221, M_{male} = 5.288, SD_{male} = 1.249, t(704) = 0.622, p = 0.534). In addition, a regression analysis suggested that age was positively related to privacy concerns (B = 0.131, SE = 0.041, t = 3.215, p = 0.001). In terms of privacy behaviour, the results from independent sample *t*-tests reveal that there was no difference between males and females in reactive behaviour (M_{female} = 4.331, SD_{female} = 1.600, M_{male} = 4.518, SD_{male} = 1.753, t(704) = 1.481, p = 0.139). However, males were more likely to engage in proactive behaviour than females (M_{female} = 4.838, SD_{female} = 1.296, M_{male} = 5.037, SD_{male} = 1.388, t(704) = 1.968, p = 0.049). Regression analysis suggested that age did not have a significant effect on reactive privacy behaviour (B = 0.065, SE = 0.056, t = 1.165, p = 0.245) but was positively related to proactive privacy behaviour (B = 0.169, SE = 0.044, t = 3.819, p = 0.001).

Overall, the findings suggest that online users experience similar levels of privacy-related emotional exhaustion regardless of age and gender. In spite of no significant difference in privacy concerns and reactive protection behaviour between genders, males tend to engage more in proactive privacy protection measures, possibly because of their greater use of privacy-enhancing technologies. Additionally, older individuals show higher levels of privacy concerns and are more likely to adopt proactive protection measures, consistent with prior research indicating that age correlates positively with privacy concerns and proactive behaviour (Goldfarb and Tucker, 2012).

Main model testing

To effectively analyse these complex interactions, the study uses structural equation modelling (SEM) to test the hypotheses. SEM is a powerful statistical technique that facilitates the specification, estimation and testing of theoretical models comprising both observed and latent (unobserved) variables (Byrne, 2001; Kaplan, 2009). This method is particularly well-suited for the current study, as it allows for the examination of both direct and indirect relationships among multiple variables (Hair, Black, Babin, Anderson, and Tatham, 2006). This capability is essential for testing the proposed model, especially in assessing how privacy concerns mediate relationships among variables and how emotional exhaustion moderates various pathways within the model. SEM, therefore, provides a robust framework for understanding the complex dynamics that influence online well-being.

Shook *et al*. (2004, p. 397) describe SEM as "a set of linear equations that simultaneously test two or more relationships among directly observable and/or unmeasured latent variables". This method allows researchers to assess model fit and rigorously test theoretically derived and *a priori* specified causal hypotheses (Voss, 2023). The advantages of SEM include its ability to simultaneously examine a series of dependence relationships, incorporate multiple independent variables, mediators and dependent variables (Voss, 2023), account for measurement errors and other sources of error (Bagozzi *et al*., 1998), empirically test theoretical measurement models and hypotheses (Chin, 1998), and provide simultaneous

estimation (Iacobucci *et al.*, 2007). Furthermore, covariance-based SEM stands out as a powerful tool for researchers, offering a comprehensive approach to assessing and refining theoretical models (Anderson and Gerbing, 1988, p. 411). Notably, SEM exhibits robustness even in the presence of violations of underlying distributional assumptions, enhancing its reliability and applicability in various research contexts (Reinartz *et al.*, 2009, p. 332).

In terms of sample size, SEM typically requires a relatively large number of participants to ensure robust and reliable results. According to Kaplan (2009) and Raykov and Marcoulides (2000), a sample size of 200–400 is generally considered adequate for models with 10–15 indicators. As a general guideline, Loehlin (1992) suggests that the minimum sample size should be at least 50 plus eight times the number of variables in the model. Mitchell (1993) recommends a ratio of 20 cases per variable, while Stevens (1996) advises a subject-to-predictor ratio of 15:1. Given that this study includes 22 observed variables, the minimum sample size would be 226 according to Loehlin (1992), 440 according to Mitchell (1993), and 330 according to Stevens (1996). Therefore, with a sample size of 706 participants, our study comfortably exceeds these minimum requirements, ensuring that the analysis is well-supported by a sufficient number of cases.

The fit indices for this structural model are as follows: $\chi^2(202) = 723.726$, $p < 0.001$, SRMR = 0.057, RMSEA = 0.061, CFI = 0.936, Tucker-Lewis Index = 0.920 and GFI = 0.917. These results suggest a good fit between the model and the data. The results support four of our six hypothesised relationships (Table 4). Overall, vulnerability was positively related to privacy concerns, which increased both reactive and proactive privacy protection. However, only proactive privacy protection positively and significantly influenced online well-being. Therefore, *H1*, *H3a*, *H3b* and *H5* are supported, and *H2* and *H4* were not supported. Additional analysis reveals that the indirect effect of data vulnerability on online subjective well-being via privacy concerns and proactive behaviour was significant ($b = 0.0354$, se = 0.0080, 90%CI [0.0211, 0.0525]).

Among the control variables, only the effects of age on privacy concerns and education on reactive privacy protection were significant. Specifically, the older the respondents were, the more likely they were to be concerned about privacy. In addition, greater education increased reactive privacy protection behaviour.

Privacy emotional exhaustion as a moderator

Following Cheah *et al.* (2020) and Little *et al.* (2006), we adopted the orthogonalised approach to test the moderation effects of privacy emotional exhaustion. First, the uncentered emotional exhaustion indicators were multiplied with the uncentered indicators of each of the independent variables (i.e. vulnerability and privacy concerns) to form indicators for the corresponding interaction variables. For each interaction variable, new residual-based indicators were created from the residuals of the regression of all exogenous indicators on each of the new corresponding interactive variable indicators. The regression residuals were used as measures of each of the respective latent interaction variables. In the second step, the moderator and interactive terms were included in the model. The residuals of the product indicators of each of the latent interaction variables were covaried based on the guidelines of Cheah *et al.* (2020) and Little *et al.* (2006) to make sure that there was no shared variance between the indicators of the interaction term and the indicators of the independent variable and the moderator. The results are provided in Table 5.

It was found that the interaction term between emotional exhaustion and data vulnerability had a significant effect on privacy concerns and well-being. In addition, the interaction term between emotional exhaustion and privacy concerns had a significant effect on reactive protection behaviour but not proactive protection behaviour. Therefore, *H6*, *H7*

Table 4. Results regarding the main effects

Structural paths	Predicted direction of effect	β	t-value	Significance level	Hypothesis	Findings
Hypothesised relationship						
Vulnerability → privacy concerns	+	0.590	14.230	***	*H1*	Supported
Vulnerability → online well-being	−	−0.070	−1.733	0.083	*H2*	Not supported
Privacy concerns → reactive privacy protection	+	0.712	15.921	***	*H3a*	Supported
Privacy concerns → proactive privacy protection	+	0.740	15.530	***	*H3b*	Supported
Reactive privacy protection → online well-being	−	0.021	0.410	0.682	*H4*	Not supported
Proactive privacy protection → online well-being	+	0.523	8.948	***	*H5*	Supported
Control variables						
Age → privacy concerns	N/A	0.078	2.177	*	Control	N/A
Gender → privacy concerns	N/A	−0.008	−0.230	0.818	Control	N/A
Education → privacy concerns	N/A	0.053	1.431	0.152	Control	N/A
Income → privacy concerns	N/A	−0.023	−0.621	0.535	Control	N/A
Age → reactive privacy protection	N/A	−0.060	−1.879	0.060	Control	N/A
Gender → reactive privacy protection	N/A	0.039	1.229	0.219	Control	N/A
Education → reactive privacy protection	N/A	0.137	4.190	***	Control	N/A
Income → reactive privacy protection	N/A	0.024	0.740	0.460	Control	N/A
Age → proactive privacy protection	N/A	0.050	1.481	0.139	Control	N/A
Gender → proactive privacy protection	N/A	0.064	1.884	0.060	Control	N/A
Education → proactive privacy protection	N/A	0.046	1.332	0.183	Control	N/A
Income → proactive privacy protection	N/A	0.035	1.332	0.183	Control	N/A
Age → online well-being	N/A	−0.003	−0.074	0.941	Control	N/A
Gender → online well-being	N/A	0.042	1.029	0.303	Control	N/A
Education → online well-being	N/A	−0.058	−1.524	0.128	Control	N/A
Income → online well-being	N/A	0.051	1.362	0.173	Control	N/A

Notes(s): ***$p < 0.001$, *$p < 0.05$
Source(s): Authors' own work

Table 5. Results regarding moderating effects (standardised regression weight on DV)

IV	DV[a]	*B* (IV[b])	*β* (MOD[c])	*β* (IAT[d])
Vulnerability	Privacy concerns	0.479***	0.090+	0.084*
Vulnerability	Online well-being	−0.130*	−0.266***	0.262***
Privacy concerns	Reactive privacy protection	0.450***	0.479***	0.104***
Privacy concerns	Proactive privacy protection	0.632***	0.184***	0.019+

Notes: [a]DV = dependent variable; [b]IV = independent variable; [c]MOD = moderator; [d]IAT = interaction term; +not sig., *$p < 0.05$; ***$p < 0.001$
Source(s): Authors' own work

and *H8* were supported. In general, as customers become more emotionally exhausted about privacy, their level of data vulnerability will have a stronger effect on privacy concerns and a weaker effect on online well-being; in addition, as the level of emotional exhaustion increases, the effect of privacy concerns on reactive protection behaviour (but not proactive behaviour) will become stronger (Figures 2, 3 and 4). The following section provides a detailed discussion of our findings.

Discussion

The current study extends the APCO theory by incorporating subjective (online) well-being as a consequence. The results, although not directly, reveal insights into the renowned debates of the privacy paradox by considering the role of emotional exhaustion. Furthermore, a novel tension (thereby exhaustion tension) undocumented in literature was found on how privacy concerns prompt emotionally exhausted consumers to exercise more reactive (active) but not proactive (passive) protection decisions. Last but not least, we revealed the disparate influences of protection behaviours (i.e. reactive and proactive) on online well-being. These insights collectively address the overarching research question: What mechanism underlies the impact of data vulnerability on consumers' privacy protection behaviour and online subjective well-being?

The findings confirmed that data vulnerability magnifies privacy concerns (*H1*). Our result corroborates the finding of Smith *et al.* (2011) that users' privacy concerns are aggravated in the presence of privacy events or abuses. While firms' exploitation of personal

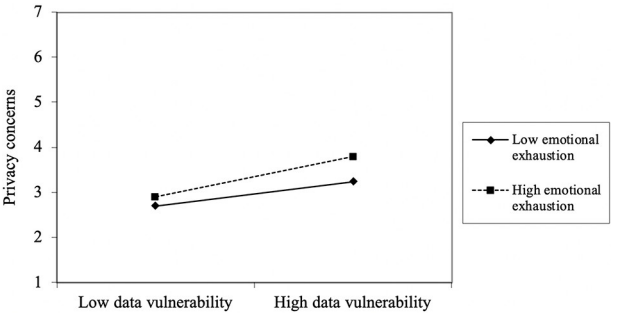

Figure 2. Moderating effect of privacy emotional exhaustion on the relationship between vulnerability and privacy concerns
Source: Authors' own work

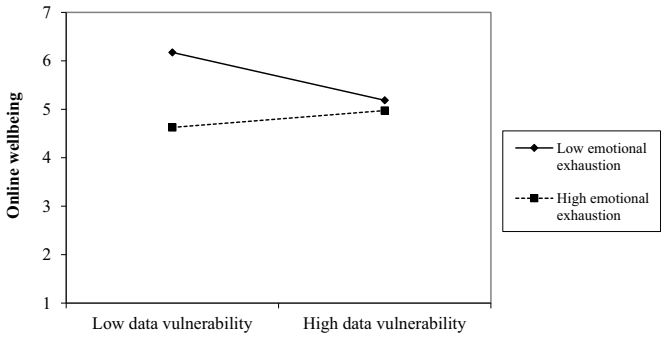

Figure 3. Moderating effect of privacy emotional exhaustion on the relationship between vulnerability and online well-being
Source: Authors' own work

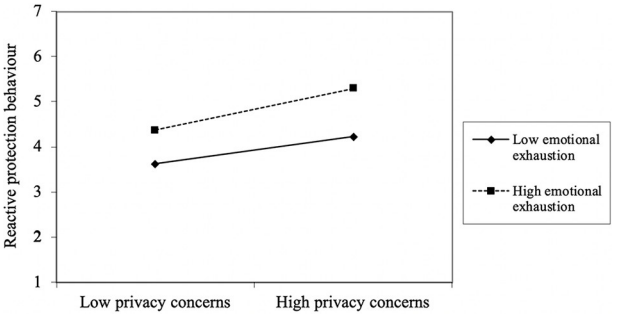

Figure 4. Moderating effect of privacy emotional exhaustion on the relationship between privacy concerns and reactive protection behaviour
Source: Authors' own work

data has increasingly become a norm, most consumers still have limited or no strategies to safeguard themselves from privacy threats (Young and Quan-Haase, 2013). We further supported the importance of consumers' perception of vulnerability, supporting earlier research highlighting concerns evoked from consumers' understanding of the state of their privacy regardless of actual data breach experience (Palmatier and Martin, 2019).

Although the statistical results for the relationship between data vulnerability and online well-being (*H2*) are not significant ($p = 0.083$), the observed negative relationship hints at a psychological impact on consumers' well-being as an indirect consequence of their feelings of vulnerability. This suggests that data vulnerability affects online subjective well-being through a mediating mechanism involving privacy concerns and proactive (but not reactive) behaviour. This finding aligns with the APCO model, which outlines the sequential relationship between data vulnerability, privacy concerns, proactive protection behaviour and online subjective well-being.

Our findings align with prior research that emphasises the indirect impact of data vulnerability on various privacy-related outcomes. For example, Martin *et al.* (2017) demonstrated the indirect effects of data vulnerability on privacy behaviours such as

falsifying information, negative word-of-mouth and switching, mediated by perceptions of violation and trust. Their research underscores the pivotal role of data vulnerability in shaping consumer responses to firms' information practices, highlighting its significance beyond direct privacy concerns or financial implications. Similarly, Liu *et al.* (2023) revealed the indirect effect of data vulnerability on consumers' continued usage intention of sharing accommodation platforms. Their study indicated that consumer data vulnerability positively influences privacy concerns, subsequently leading to a negative impact on continued platform usage. This suggests that individuals are more likely to respond unfavourably to the use of their data when they perceive heightened privacy concerns. Moreover, research by Tucker (2014) suggests that individuals exhibit more favourable responses to data usage when they have control over their personal privacy settings, indicative of lower privacy concerns. Our findings further extend this understanding by highlighting the indirect effect of data vulnerability on online subjective well-being through privacy concerns and proactive protection behaviour. Eventually, privacy protection measures must arise to answer the urgency of consumers' privacy concerns (*H3*). While existing studies have confirmed that consumers take both proactive and reactive actions to protect their privacy when concerns are heightened (Baruh *et al.*, 2017; Choi *et al.*, 2018; Yang, 2013), none have explicitly distinguished or considered both behaviours simultaneously. Our study, therefore, adds value by advancing understanding and highlighting the need to consider both behaviours within the same context.

Contrary to the common expectation that privacy protection alleviates anxiety and stress, thereby enhancing life quality, our results confirmed that only proactive (*H5*), not reactive (*H4*), privacy protection behaviours positively relate to online well-being, indicating that not all protection measures yield the same effect. Although not statistically significant, reactive measures seem to have a negative effect on well-being on account of the changes in social interaction, which are central to the reactive responses (Quach *et al.*, 2022). In contrast, performing proactive protection behaviour can prevent future privacy problems (Chou and Chou, 2021), which can lead to peace of mind and overall satisfaction with life.

Regarding emotional exhaustion – a pivotal component of the fatigue concept – fatigue literature suggested that emotionally depleted people tend to be reluctant to go any further or unable to make privacy decisions (Ream and Richardson, 1996; Shao *et al.*, 2022) and are more likely to do nothing in response to their personal information misuse (Choi *et al.*, 2018; Shao *et al.*, 2022; van Ooijen *et al.*, 2022). Our study found that emotional exhaustion increased the impact of data vulnerability on privacy concerns (*H6*). It also amplified the effect of privacy concerns on reactive, but not proactive, protection behaviours (*H8*). Emotionally exhausted consumers would exhibit more privacy concerns when their vulnerability increases, and their concerns are more likely to translate into reactive protection behaviours. Our findings underscore the heightened mental burden faced by modern consumers (Bright *et al.*, 2021). We highlight how high privacy demands and limited cognitive resources contribute to burnout and anxiety, emphasising the role of emotional exhaustion (Choi *et al.*, 2018) within the broader context of psychological well-being. Unlike privacy cynicism, which reflects frustration, hopelessness and disillusionment because of unmet expectations, emotional exhaustion in our study pertains to the fatigue that arises from constant privacy demands. This indicates that emotional exhaustion is one of the key mechanisms underpinning the privacy paradox (Agozie and Kaya, 2021; Choi *et al.*, 2018; Tang *et al.*, 2021). Furthermore, the impact of vulnerability on consumers' well-being is weaker in the presence of high emotional exhaustion (*H7*). Previous research found that the negative impact of vulnerability gradually decreased to a point where privacy intrusions no longer caused negative feelings (Oulasvirta *et al.*, 2012). We further provided evidence to

enrich existing findings, demonstrating that high emotional exhaustion mitigates the negative effect of privacy vulnerability on the end-state outcome of online well-being.

Finally, concerning demographic differences, the findings demonstrate that online users experience the same level of privacy and emotional exhaustion regardless of their age and gender. Furthermore, although extant studies such as Bartel Sheehan (1999) and Hoy and Milne (2010) found a significant relationship between gender and privacy concerns, our results support Jensen *et al.* (2005) and Yao *et al.* (2007), which suggest that the effect of gender on privacy concerns is inconclusive and may be contingent on specific contexts, such as social media. In spite of exhibiting no difference in privacy concerns and reactive privacy protection behaviour, males were more likely to engage in proactive privacy protection behaviour. This inclination could be attributed to the fact that proactive measures often involve using privacy-enhancing technologies, and males are more likely to leverage technology as tools for privacy protection compared to females (Hoy and Milne, 2010). It is worth noting that proactive protection involves preventive measures, typically uzing privacy-enhancing technologies, while reactive protection entails actions in response to a privacy incident, applicable to any affected individual (Chou and Chou, 2021). Finally, our results indicate a positive correlation between age and privacy concerns, as well as a tendency for older respondents to adopt proactive privacy protection measures. This aligns with previous research, such as the work of Goldfarb and Tucker (2012), suggesting that as individuals age, they become more conscious of privacy issues and are more proactive in safeguarding their online privacy. Building on the results, the next section provides insights into theoretical and practical implications.

Implications

Theoretical implications

The study contributes to the emerging literature on online subjective well-being and consumers' privacy in several ways. First, bridging the privacy literature and subjective well-being literature, the current study extends the ACPO model by incorporating data vulnerability as an antecedent of privacy concerns and online well-being as the ultimate outcome. Whereas the majority of current research examines subjective online well-being from the perspective of social media use (Verduyn *et al.*, 2017), our study offers evidence of the impact of overall data vulnerability and privacy responses on customers' subjective online well-being. This study supports earlier research such as Rahman (2021), who postulates that individual-driven sources are among the key factors that influence satisfaction with life (i.e. online well-being). The paper also enhances understanding of the ultimate psychological benefits of privacy protection behaviours, namely, online well-being (Palmatier and Martin 2019). Furthermore, we contribute to the discourse on the privacy/vulnerability tradeoffs identified by Martin *et al.* (2017) by delineating the boundary conditions that intensify the impact of data vulnerability on consumers, particularly when they are experiencing emotional exhaustion. Under these circumstances, individuals are more likely to adopt reactive protection behaviours as opposed to proactive strategies.

Second, we provide evidence to support the significant and positive impacts of proactive rather than reactive protection behaviours on consumers' subjective online well-being, extending existing privacy research such as Martin *et al.* (2017) and Quach *et al.* (2022). Specifically, drawing on the privacy protection typology outlined by Quach *et al.* (2022), our study represents the first empirical endeavour to operationalise the distinctions between proactive and reactive protection behaviours. Unlike many prior privacy studies that often focus solely on one type of protection behaviour (e.g. Soomro and Hussain, 2019; Yang, 2013) or fail to clearly distinguish between proactive and reactive behaviours (e.g.

Wisniewski *et al.*, 2015), our research underscores the importance of considering these distinctions. By recognising the disparate effects of proactive and reactive protection behaviours, our study emphasises the need for a nuanced approach when investigating consumers' privacy concerns and subjective online well-being. This understanding is crucial for developing targeted interventions and strategies aimed at enhancing individuals' online experiences and well-being. In addition, we also shed light on the conditions influencing consumers' selection of protective actions, thereby elucidating their impact on online well-being as a consequential effect of privacy-related decisions. Our findings provide compelling evidence supporting the significant and positive impacts of proactive protection behaviours on consumers' subjective online well-being. This innovative approach not only expands the insights provided by Quach *et al.* (2022) and Martin *et al.* (2017) but also paves the way for exploring a wider range of consequences stemming from privacy-related decisions.

Finally, this study extends the current understanding of privacy tension in the presence of emotional exhaustion. Recent studies corroborated that emotional exhaustion is one of the key mechanisms behind the privacy paradox (Augustin *et al.*, 2022; Choi *et al.*, 2018; Pomfret *et al.*, 2020). Emotionally exhausted consumers are more likely to avoid coping measures and engage in non-protective behaviours (e.g. self-disclosure). Our findings suggest that among emotionally exhausted consumers, high privacy concerns translate into reactive protection measures but not proactive ones on account of reservation efforts (Levav *et al.*, 2010). Individuals who prioritise privacy often exhibit different responses to immediate threats, with some leaning towards reactive behaviour. Reactive behaviour involves addressing issues as they arise rather than taking proactive steps to prevent them. Conversely, these individuals may hesitate to engage in proactive behaviour, which entails taking preemptive measures to safeguard their privacy. This reluctance towards proactive measures can be attributed to their preventive nature, where the potential benefits, being uncertain and not immediate, may not seem to outweigh the costs. Consequently, the perceived advantages of proactive protection may not convincingly outweigh its associated expenses, thus limiting its impact.

Practical implications

Several practical implications emerge from the study results. First, privacy concerns play a central role in the relationship between vulnerability, behavioural responses (i.e. protection behaviours) and consumers' well-being. The positive correlation between privacy concerns and both reactive and proactive protection behaviours confirms that consumers are likely to embark on different privacy paths (i.e. proactive and reactive) consistent with findings from the Helsinki experiment. However, only proactive protection measures result in subjective well-being. This reflects the tumultuous digital world where preventive, not remedial, responses are preferable. Customers need to be encouraged to engage in more proactive behaviour instead of reacting only after an incident happens. To bolster proactive privacy protection, businesses should implement several key strategies. First, they should develop user-friendly privacy controls, including intuitive dashboards that allow users to easily manage privacy settings and data-sharing preferences (Grünewald *et al.*, 2023). Robust default privacy settings, combined with granular customisation options, will further empower users. Regular internal and third-party privacy audits are crucial for identifying and addressing vulnerabilities and ensuring compliance with industry standards.

Additionally, businesses should adopt privacy by design and rights management practices (Abomhara *et al.*, 2024). Privacy by default, embedded in IT systems and business practices, ensures automatic protection of user privacy without requiring user intervention. Rights management software can aid users in visualising and exercising their privacy controls, allowing

them to edit, download, share and toggle privacy settings as needed. Advanced digital fingerprinting techniques can be used to track intruders with details such as date, time, username and email, deterring screenshot data theft. By preventing breaches and enhancing preventive measures, businesses can significantly reduce customer vulnerability, promote proactive privacy protection and improve overall online well-being.

Moreover, our study extends beyond the scope of previous research, such as Martin *et al.* (2017), by offering actionable insights into the role of emotional exhaustion and its implications for consumer behaviour. Consumers' irrational evaluations and behaviours are influenced by emotional exhaustion, highlighting the need for tailored approaches to enhance their well-being in the context of data vulnerability and privacy concerns. Overexploiting users' information and data breaches would likely induce mental fatigue, which represses user enthusiasm for protection measures (Maslach *et al.*, 2001) This poses a significant risk to businesses reliant on personal data, jeopardising the value derived from such information (Tang *et al.*, 2021). Additionally, overly complex privacy policies can contribute to emotional exhaustion, further exacerbating the issue. To mitigate emotional exhaustion and promote user well-being, firms should prioritise transparency and user empowerment in their privacy practices. This includes using clear and concise language in privacy policies, simplifying privacy options and empowering users to control their privacy settings. For example, firms can adopt measures such as turning off non-essential cookies by default and implementing active opt-in mechanisms for data collection. Furthermore, offering incentives such as digital discount vouchers or monetary rewards (e.g. crypto tokens) in exchange for user consent to track basic information, with an opt-out option readily available, can help foster a more collaborative and transparent approach to privacy management without triggering emotional exhaustion.

Conclusion, limitations and future research directions

The current study investigates the relationship between data vulnerability, privacy concerns, privacy protection behaviours and subjective online well-being in the presence of privacy emotional exhaustion. Though the study offers important implications, there are several limitations. First, we used cross-sectional data in this study, which only captured a "snapshot" of the phenomena of interest at a specific time. As the digital environment is rapidly changing with emerging technologies and data protection regulations, a longitudinal study will be beneficial to understand the evolution of privacy. Furthermore, the APCO model could be extended to embed other privacy calculus constructs such as trust, risks/costs and perceived benefits (Dinev *et al.*, 2015), along with self-efficacy, response-efficacy, or privacy literacy.

Another limitation arises from the use of MTurk for data collection. While using MTurk for data collection offers significant efficiency advantages for researchers (Goodman and Paolacci, 2017), it also presents several challenges related to generalisability. MTurk participants tend to be younger and more educated, which may not accurately reflect the broader population of internet users (Chandler *et al.*, 2019). Additionally, participants' motivations, often driven by monetary incentives, could introduce bias, potentially affecting the authenticity of their responses. While quality control measures were implemented to mitigate these concerns, future research should compare MTurk results with data from other sources or methods to assess the robustness and generalisability of the findings. Incorporating alternative recruitment platforms or sampling methods could help improve the diversity and representativeness of the participant pool.

Furthermore, all research participants in the main study were consumers from the USA. Given that cultural differences can significantly influence privacy attitudes and behaviours

(Chen *et al.*, 2013), future research should validate these findings in other cultural contexts. Specifically, investigating how cross-cultural or cross-national variations in privacy concerns shape attitudes and behaviours (Martin *et al.*, 2017) would provide valuable insights into privacy dynamics. It would also be valuable to explore how consumers in different cultures perceive their vulnerability to privacy violations, especially in societies where privacy may not be a top priority. Additionally, examining how varying levels of data vulnerability and emotional exhaustion impact privacy protection behaviours in different situations could offer important insights. Understanding the boundary conditions under which reactive and proactive privacy protection behaviours enhance subjective online well-being is another promising avenue for future research.

Several key research areas remain underexplored and warrant further investigation to advance the understanding of digital privacy management, consumer protection strategies and online well-being. One important area is the psychological mechanisms that influence privacy protection behaviours. Cognitive biases, such as optimism bias, may cause individuals to underestimate privacy risks, leading to a preference for reactive over proactive protection measures (Cho *et al.*, 2010). Moreover, personality traits play a role in privacy decision-making, as individuals high in agreeableness tend to exhibit greater privacy concerns (Korzaan and Boswell, 2008), while those high in neuroticism may engage in more structured privacy protection behaviours because of perceived vulnerability and severity (Chennamaneni and Gupta, 2023). To address this, future research could explore questions such as: *How do cognitive biases (e.g. optimism bias) shape proactive vs reactive privacy protection?* and *What* role *do personality traits play in privacy decision-making?*

The temporal evolution of privacy concerns is another area requiring attention. Privacy concerns are not static; they fluctuate over time, particularly with repeated exposure to data vulnerability incidents, often leading to privacy fatigue and reduced protective behaviours (Choi *et al.*, 2018). At the same time, increasing digital literacy and shifts in data protection regulations can influence privacy coping strategies (Lyu *et al.*, 2024) by giving consumers more control over their personal data. This opens up several important research questions, such as: *How do privacy concerns fluctuate over time with repeated exposure to data vulnerability?* and *How do digital literacy and regulatory shifts impact privacy coping strategies?*

Contextual differences in privacy behaviours also need further exploration, particularly in relation to cultural norms. Privacy concerns and coping mechanisms vary across societies with different privacy expectations. For instance, individuals in collectivist cultures may prioritise privacy risks to protect the collective, whereas those in individualist cultures may focus more on personal control and freedom (Li *et al.*, 2022; Trepte *et al.*, 2017). Regulatory environments, such as the EU's General Data Protection Regulation (GDPR), enforce stringent privacy protections, leading to different privacy behaviours compared to more self-regulatory environments such as the USA. To understand these variations, research should address questions such as: *How do privacy concerns and coping mechanisms differ across cultures with varying privacy norms?*

Finally, the role of organisational responsibility in privacy protection remains an open question. Surprisingly, privacy policies, while potentially increasing emotional exhaustion, which influences privacy fatigue (Agozie and Kaya, 2021), can also be effective in mitigating privacy concerns, particularly when implemented through privacy-by-design principles and ethical AI practices (Zhu *et al.*, 2021). Further research is needed to determine how firms can develop transparency tools that minimise privacy-related stress and what regulatory frameworks are most effective in ensuring ethical and consumer-centric privacy protection. Key questions for future studies include: *How can firms design transparency*

tools to mitigate privacy-related emotional exhaustion? and *What regulatory frameworks are necessary to ensure ethical and consumer-centric privacy protection?* Addressing these research areas will further advance theoretical and practical understanding of digital privacy management, consumer protection strategies and online well-being.

References

Abomhara, M., Nweke, L.O., Yayilgan, S.Y., Comparin, D., Teyras, K. and de Labriolle, S. (2024), "Enhancing privacy protections in national identification systems: an examination of stakeholders' knowledge, attitudes, and practices of privacy by design", *International Journal of Information Security*, Vol. 23 No. 6, pp. 1-25.

Acquisti, A. and Grossklags, J. (2005), "Privacy and rationality in individual decision making", *IEEE Security and Privacy Magazine*, Vol. 3 No. 1, pp. 26-33, doi: 10.1109/MSP.2005.22.

Acquisti, A., John, L.K. and Loewenstein, G. (2013), "What is privacy worth?", *The Journal of Legal Studies*, Vol. 42 No. 2, pp. 249-274, doi: 10.1086/671754.

Agozie, D.Q. and Kaya, T. (2021), "Discerning the effect of privacy information transparency on privacy fatigue in e-government", *Government Information Quarterly*, Vol. 38 No. 4, p. 101601, doi: 10.1016/j.giq.2021.101601.

Aguinis, H., Villamor, I. and Ramani, R.S. (2021), "MTurk research: review and recommendations", *Journal of Management*, Vol. 47 No. 4, pp. 823-837.

Anderson, J.C. and Gerbing, D.W. (1988), "Structural equation modeling in practice: a review and recommended two-step approach", *Psychological Bulletin*, Vol. 103 No. 3, p. 411.

Augustin, Y., Carolus, A. and Wienrich, C. (2022), "Privacy of AI-based voice assistants: Understanding the users' perspective", *Design, Operation and Evaluation of Mobile Communications, Cham*.

Azizan, N.H. and Mahmud, Z. (2018), "Determinants of subjective wellbeing: a systematic review", *6th AMER International Conference on Quality of Life, Malaysia*.

Bagozzi, R.P., Yi, Y. and Nassen, K.D. (1998), "Representation of measurement error in marketing variables: Review of approaches and extension to three-facet designs", *Journal of Econometrics*, Vol. 89 Nos 1-2, pp. 393-421.

Bandara, R., Fernando, M. and Akter, S. (2021), "Managing consumer privacy concerns and defensive behaviours in the digital marketplace", *European Journal of Marketing*, Vol. 55 No. 1, pp. 219-246, doi: 10.1108/EJM-06-2019-0515.

Bartel Sheehan, K. (1999), "An investigation of gender differences in on-line privacy concerns and resultant behaviours", *Journal of Interactive Marketing*, Vol. 13 No. 4, pp. 24-38.

Baruh, L., Secinti, E. and Cemalcilar, Z. (2017), "Online privacy concerns and privacy management: a Meta-Analytical review", *Journal of Communication*, Vol. 67 No. 1, pp. 26-53, doi: 10.1111/jcom.12276.

Bright, L.F., Lim, H.S. and Logan, K. (2021), "'Should I post or ghost?': Examining how privacy concerns impact social media engagement in US consumers", *Psychology and Marketing*, Vol. 38 No. 10, pp. 1712-1722.

Buck, C., Dinev, T. and Anaraky, R.G. (2022), "Revisiting APCO", in Knijnenburg, B.P., Page, X., Wisniewski, P., Lipford, H.R., Proferes, N. and Romano, J. (Eds), *Modern Socio-Technical Perspectives on Privacy*, Springer International Publishing, pp. 43-60, doi: 10.1007/978-3-030-82786-1_3.

Byrne, B.M. (2001), "Structural equation modeling: perspectives on the present and the future", *International Journal of Testing*, Vol. 1 No. 3, pp. 327-334.

Chae, H.-C., Kim, G. and Koh, C.E. (2022), "Impact of privacy behaviors on relatedness and wellbeing in SNSs", *Journal of Computer Information Systems*, Vol. 63 No. 1, pp. 1-12, doi: 10.1080/08874417.2022.2052378.

Chandler, J., Rosenzweig, C., Moss, A.J., Robinson, J. and Litman, L. (2019), "Online panels in social science research: expanding sampling methods beyond mechanical Turk", *Behavior Research Methods*, Vol. 51 No. 5, pp. 2022-2038.

Cheah, J.H., Thurasamy, R., Memon, M.A., Chuah, F. and Ting, H. (2020), "Multigroup analysis using SmartPLS: step-by-step guidelines for business research", *Asian Journal of Business Research*.

Chen, H.-T. and Li, X. (2017), "The contribution of mobile social media to social capital and psychological wellbeing: examining the role of communicative use, friending and self-disclosure", *Computers in Human Behavior*, Vol. 75, pp. 958-965, doi: 10.1016/j.chb.2017.06.011.

Chen, R., Fung, B.C., Mohammed, N., Desai, B.C. and Wang, K. (2013), "Privacy-preserving trajectory data publishing by local suppression", *Information Sciences*, Vol. 231, pp. 83-97.

Chennamaneni, A. and Gupta, B. (2023), "The privacy protection behaviours of the mobile app users: exploring the role of neuroticism and protection motivation theory", *Behaviour and Information Technology*, Vol. 42 No. 12, pp. 2011-2029, doi: 10.1080/0144929X.2022.2106307.

Chin, W.W. (1998), "Commentary: issues and opinion on structural equation modeling", *MIS Quarterly*, pp. vii-xvi.

Cho, H., Lee, J.-S. and Chung, S. (2010), "Optimistic bias about online privacy risks: testing the moderating effects of perceived controllability and prior experience", *Computers in Human Behavior*, Vol. 26 No. 5, pp. 987-995, doi: 10.1016/j.chb.2010.02.012.

Choi, H., Park, J. and Jung, Y. (2018), "The role of privacy fatigue in online privacy behaviour", *Computers in Human Behavior*, Vol. 81, pp. 42-51, doi: 10.1016/j.chb.2017.12.001.

Chou, H.-L. and Chou, C. (2021), "How teens negotiate privacy on social media proactively and reactively", *New Media and Society*, Vol. 25 No. 6, p. 14614448211018797, doi: 10.1177/14614448211018797.

Cloarec, J., Meyer-Waarden, L. and Munzel, A. (2022), "The personalization–privacy paradox at the nexus of social exchange and construal level theories", *Psychology and Marketing*, Vol. 39 No. 3, pp. 647-661, doi: 10.1002/mar.21587.

Cropanzano, R., Rupp, D.E. and Byrne, Z.S. (2003), "The relationship of emotional exhaustion to work attitudes, job performance, and organizational citizenship behaviours", *Journal of Applied Psychology*, Vol. 88 No. 1, pp. 160-169, doi: 10.1037/0021-9010.88.1.160.

Davis, T.R.V. and Luthans, F. (1980), "A social learning approach to organizational behavior", *The Academy of Management Review*, Vol. 5 No. 2, pp. 281-290, doi: 10.5465/amr.1980.4288758.

De Wolf, R. (2020), "Contextualizing how teens manage personal and interpersonal privacy on social media", *New Media and Society*, Vol. 22 No. 6, pp. 1058-1075, doi: 10.1177/1461444819876570.

Dienlin, T. and Johannes, N. (2020), "The impact of digital technology use on adolescent wellbeing", *Dialogues in Clinical Neuroscience*, Vol. 22 No. 2, pp. 135-142.

Dienlin, T. and Trepte, S. (2015), "Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviours", *European Journal of Social Psychology*, Vol. 45 No. 3, pp. 285-297, doi: 10.1002/ejsp.2049.

Dinev, T., McConnell, A.R. and Smith, H.J. (2015), "Research commentary–informing privacy research through information systems, psychology, and behavioral economics: Thinking outside the 'APCO' box", *Information Systems Research*, Vol. 26 No. 4, pp. 639-655, doi: 10.1287/isre.2015.0600.

Dinev, T., Xu, H., Smith, J.H. and Hart, P. (2013), "Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts", *European Journal of Information Systems*, Vol. 22 No. 3, pp. 295-316, doi: 10.1057/ejis.2012.23.

Erfani, S.S. and Abedin, B. (2018), "Impacts of the use of social network sites on users' psychological wellbeing: a systematic review", *Journal of the Association for Information Science and Technology*, Vol. 69 No. 7, pp. 900-912, doi: 10.1002/asi.24015.

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

Goldfarb, A. and Tucker, C. (2012), "Shifts in privacy concerns", *American Economic Review*, Vol. 102 No. 3, pp. 349-353.

Goodman, J.K. and Paolacci, G. (2017), "Crowdsourcing consumer research", *Journal of Consumer Research*, Vol. 44 No. 1, pp. 196-210.

Grünewald, E., Halkenhäußer, J.M., Leschke, N., Washington, DC, J., Paupini, C. and Pallas, F. (2023) "Enabling versatile privacy interfaces using machine-readable transparency information", *Privacy Symposium: Data Protection Law International Convergence and Compliance with Innovative Technologies*, Springer International Publishing, Cham, pp. 119-137.

Guest, G., Namey, E.E. and Mitchell, M.L. (2013), *Collecting Qualitative Data: A Field Manual for Applied Research*, Sage.

Hair, J.F., Black, W.C., Babin, B.J., Anderson, R.E. and Tatham, R.L. (2006), *SEM: Confirmatory Factor Analysis. Multivariate Data Analysis*, Pearson Prentice Hall, Upper Saddle River, pp. 770-842.

Hoy, M.G. and Milne, G. (2010), "Gender differences in privacy-related measures for young adult facebook users", *Journal of Interactive Advertising*, Vol. 10 No. 2, pp. 28-45.

Iacobucci, D., Saldanha, N. and Deng, X. (2007), "A meditation on mediation: evidence that structural equations models perform better than regressions", *Journal of Consumer Psychology*, Vol. 17 No. 2, pp. 139-153.

Janakiraman, R., Lim, J.H. and Rishika, R. (2018), "The effect of a data breach announcement on customer behavior: evidence from a multichannel retailer", *Journal of Marketing*, Vol. 82 No. 2, pp. 85-105, doi: 10.1509/jm.16.0124.

Jensen, C., Potts, C. and Jensen, C. (2005), "Privacy practices of internet users: self-reports versus observed behaviour", *International Journal of Human-Computer Studies*, Vol. 63 No. 1-2, pp. 203-227.

Kaplan, D. (2009), *Structural Equation Modeling: Foundations and Extensions*, (2nd ed.), SAGE, Thousand Oaks, CA.

Kaur, P., Islam, N., Tandon, A. and Dhir, A. (2021), "Social media users' online subjective wellbeing and fatigue: a network heterogeneity perspective", *Technological Forecasting and Social Change*, Vol. 172, p. 121039, doi: 10.1016/j.techfore.2021.121039.

Kokolakis, S. (2017), "Privacy attitudes and privacy behaviour: a review of current research on the privacy paradox phenomenon", *Computers and Security*, Vol. 64, pp. 122-134, doi: 10.1016/j.cose.2015.07.002.

Korzaan, M.L. and Boswell, K.T. (2008), "The influence of personality traits and information privacy concerns on behavioral intentions", *Journal of Computer Information Systems*, Vol. 48 No. 4, pp. 15-24, doi: 10.1080/08874417.2008.11646031.

Kramer, V. and Krafft, M. (2023), "When and how information and communication technology orientation affects salespeople's role stress: the interplay of salesperson characteristics and environmental complexity", *European Journal of Marketing*, Vol. 57 No. 3, pp. 659-682, doi: 10.1108/EJM-11-2021-0917.

Kwak, Y., Kim, J., Kim, Y. and Choi, J. (2021), "Understanding digital consumers' well-being in Asia: the moderating roles of digital natives and privacy concerns", *Journal of Consumer Affairs*, Vol. 55 No. 4, pp. 1274-1291.

Labrecque, L.I., Markos, E., Swani, K. and Peña, P. (2021), "When data security goes wrong: examining the impact of stress, social contract violation, and data type on consumer coping responses following a data breach", *Journal of Business Research*, Vol. 135, pp. 559-571, doi: 10.1016/j.jbusres.2021.06.054.

Levav, J., Heitmann, M., Herrmann, A. and Iyengar, S.S. (2010), "Order in product customization decisions: evidence from field experiments", *Journal of Political Economy*, Vol. 118 No. 2, pp. 274-299, doi: 10.1086/652463.

Li, Y., Rho, E.H.R. and Kobsa, A. (2022), "Cultural differences in the effects of contextual factors and privacy concerns on users' privacy decision on social networking sites", *Behaviour and Information Technology*, Vol. 41 No. 3, pp. 655-677, doi: 10.1080/0144929X.2020.1831608.

Little, A.C., Burt, D.M. and Perrett, D.I. (2006), "What is good is beautiful: face preference reflects desired personality", *Personality and Individual Differences*, Vol. 41 No. 6, pp. 1107-1118.

Liu, T., Li, W. and Jia, X. (2023), "Consumer data vulnerability, peer privacy concerns and continued usage intention of sharing accommodation platforms: the moderating roles of perceived benefits", *Information Technology and People*, Vol. 36 No. 6, pp. 2234-2258, doi: 10.1108/ITP-05-2021-0365.

Loehlin, J.C. (1992), *Latent Variable Models: An Guideline for Sample Size Estimation Needed for Statistical Introduction to Factor, Path and Structural Analysis, Techniques Rather than Mathematical Computation*, 2 Ed Hillsdale, NJ.

Lombardi, D.B. and Ciceri, M.R. (2016), "More than defense in daily experience of privacy: the functions of privacy in digital and physical environments", *Europe's Journal of Psychology*, Vol. 12 No. 1, pp. 115-136, doi: 10.5964/ejop.v12i1.948.

Lwin, M., Wirtz, J. and Williams, J.D. (2007), "Consumer online privacy concerns and responses: a power–responsibility equilibrium perspective", *Journal of the Academy of Marketing Science*, Vol. 35 No. 4, pp. 572-585, doi: 10.1007/s11747-006-0003-3.

Lyu, T., Guo, Y. and Chen, H. (2024), "Understanding the privacy protection disengagement behaviour of contactless digital service users: the roles of privacy fatigue and privacy literacy", *Behaviour and Information Technology*, Vol. 43 No. 10, pp. 2007-2023, doi: 10.1080/0144929X.2023.2237603.

Margulis, S.T. (1977), "Conceptions of privacy: Current status and next steps", *Journal of Social Issues*, Vol. 33 No. 3, pp. 5-21, doi: 10.1111/j.1540-4560.1977.tb01879.x.

Martin, K.D., Borah, A. and Palmatier, R.W. (2017), "Data privacy: effects on customer and firm performance", *Journal of Marketing*, Vol. 81 No. 1, pp. 36-58, doi: 10.1509/jm.15.0497.

Maslach, C., Schaufeli, W.B. and Leiter, M.P. (2001), "Job burnout", *Annual Review of Psychology*, Vol. 52 No. 1, pp. 397-422, doi: 10.1146/annurev.psych.52.1.397.

Mitchell, R.J. (1993), *Path Analysis: pollination. Design and P. S. Petraitis Analysis of Ecological Experiments (Eds S.M. Scheiner and J. Gurevitch).* Chapman and Hall, New York, NY, pp. 211-231.

Norberg, P.A., Horne, D.R. and Horne, D.A. (2007), "The privacy paradox: personal information disclosure intentions versus behaviors", *Journal of Consumer Affairs*, Vol. 41 No. 1, pp. 100-126, doi: 10.1111/j.1745-6606.2006.00070.x.

Nunnally, J.C. and Bernstein, I.H. (1994), *Psychometric Theory*, (3rd ed.), McGraw-Hill, New York, NY.

Okazaki, S., Eisend, M., Plangger, K., de Ruyter, K. and Grewal, D. (2020), "Understanding the strategic consequences of customer privacy concerns: a meta-analytic review", *Journal of Retailing*, Vol. 96 No. 4, pp. 458-473.

Oulasvirta, A., Pihlajamaa, A., Perkiö, J., Ray, D., Vähäkangas, T., Hasu, T., Vainio, N. and Myllymäki, P. (2012), "Long-term effects of ubiquitous surveillance in the home", Proceedings of the 2012 ACM Conference on Ubiquitous Computing, *Pittsburgh, PA*.

Palmatier, R.W. and Martin, K.D. (2019), "The psychology of consumer privacy", in Palmatier, R.W. and Martin, K.D. (Eds), *The Intelligent Marketer's Guide to Data Privacy: The Impact of Big Data on Customer Trust*, Springer International Publishing, pp. 21-41, doi: 10.1007/978-3-030-03724-6_2.

Park, J., Kim, B. and Park, S. (2021), "Understanding the behavioral consequences of upward social comparison on social networking sites: the mediating role of emotions", *Sustainability*, Vol. 13 No. 11, p. 5781.

Pedersen, D.M. (1997), "Psychological functions of privacy", *Journal of Environmental Psychology*, Vol. 17 No. 2, pp. 147-156, doi: 10.1006/jevp.1997.0049.

Podsakoff, P.M., MacKenzie, S.B., Lee, J.-Y. and Podsakoff, N.P. (2003), "Common method biases in behavioural research: a critical review of the literature and recommended remedies", *Journal of Applied Psychology*, Vol. 88 No. 5, pp. 879-903, doi: 10.1037/0021-9010.88.5.879.

Pomfret, L., Previte, J. and Coote, L. (2020), "Beyond concern: socio-demographic and attitudinal influences on privacy and disclosure choices", *Journal of Marketing Management*, Vol. 36 Nos 5-6, pp. 519-549, doi: 10.1080/0267257X.2020.1715465.

Quach, S., Thaichon, P., Martin, K.D., Weaven, S. and Palmatier, R.W. (2022), "Digital technologies: tensions in privacy and data", *Journal of the Academy of Marketing Science*, Vol. 50 No. 6, doi: 10.1007/s11747-022-00845-y.

Rahman, A. (2021), "Sources and categories of wellbeing: a systematic review and research agenda", *Journal of Service Theory and Practice*, Vol. 31 No. 1, pp. 1-33, doi: 10.1108/JSTP-01-2020-0024.

Raykov, T. and Marcoulides, G.A. (2000), "A method for comparing completely standardized solutions in multiple groups", *Structural Equation Modeling: A Multidisciplinary Journal*, Vol. 7 No. 2, pp. 292-308.

Ream, E. and Richardson, A. (1996), "Fatigue: a concept analysis", *International Journal of Nursing Studies*, Vol. 33 No. 5, pp. 519-529, doi: 10.1016/0020-7489(96)00004-1.

Reinartz, W., Haenlein, M. and Henseler, J. (2009), "An empirical comparison of the efficacy of covariance-based and variance-based SEM", *International Journal of Research in Marketing*, Vol. 26 No. 4, pp. 332-344.

Reinecke, L. and Trepte, S. (2014), "Authenticity and wellbeing on social network sites: a two-wave longitudinal study on the effects of online authenticity and the positivity bias in SNS communication", *Computers in Human Behavior*, Vol. 30, pp. 95-102, doi: 10.1016/j.chb.2013.07.030.

Sashi, C.M. (2021), "Digital communication, value co-creation and customer engagement in business networks: a conceptual matrix and propositions", *European Journal of Marketing*, Vol. 55 No. 6, pp. 1643-1663, doi: 10.1108/EJM-01-2020-0023.

Schertzer, S., Laufer, D., Silvera, D.H. and Brad McBride, J. (2008), "A cross-cultural validation of a gender role identity scale in marketing", *International Marketing Review*, Vol. 25 No. 3, pp. 312-323.

Schwartz, B. (1968), "The social psychology of privacy", *American Journal of Sociology*, Vol. 73 No. 6, pp. 741-752, doi: 10.1086/224567.

Shao, H., Li, X. and Wang, G. (2022), "Are you tired? I am: Trying to understand privacy fatigue of social media users", *Extended Abstracts of the 2022 CHI Conference on Human Factors in Computing Systems*, *New Orleans*, *LA*. 10.1145/3491101.3519778

Shirom, A. (1989), *Burnout in Work Organizations*, Wiley.

Shook, C.L., Ketchen, D.J., Jr, Hult, G.T.M. and Kacmar, K.M. (2004), "An assessment of the use of structural equation modeling in strategic management research", *Strategic Management Journal*, Vol. 25 No. 4, pp. 397-404.

Smith, H.J., Dinev, T. and Xu, H. (2011), "Information privacy research: an interdisciplinary review", *MIS Quarterly*, Vol. 35 No. 4, pp. 989-1015, doi: 10.2307/41409970.

Smith, N.C. and Cooper-Martin, E. (1997), "Ethics and target marketing: the role of product harm and consumer vulnerability", *Journal of Marketing*, Vol. 61 No. 3, pp. 1-20, doi: 10.1177/002224299706100301.

Soomro, T.R. and Hussain, M. (2019), "Social media-related cybercrimes and techniques for their prevention", *Appl. Comput. Syst.*, Vol. 24 No. 1, pp. 9-17.

Stevens, J. (1996), *Applied Multivariate Statistics for the Social Sciences*, 3rd ed., Lawrence Erlbaum Associates, Mahwah, NJ.

Strycharz, J., van Noort, G., Helberger, N. and Smit, E. (2019), "Contrasting perspectives – practitioner's viewpoint on personalised marketing communication", *European Journal of Marketing*, Vol. 53 No. 4, pp. 635-660, doi: 10.1108/EJM-11-2017-0896.

Tang, J., Akram, U. and Shi, W. (2021), "Why people need privacy? The role of privacy fatigue in app users' intention to disclose privacy: based on personality traits", *Journal of Enterprise Information Management*, Vol. 34 No. 4, pp. 1097-1120, doi: 10.1108/JEIM-03-2020-0088.

Trepte, S., Reinecke, L., Ellison, N.B., Quiring, O., Yao, M.Z. and Ziegele, M. (2017), "A cross-cultural perspective on the privacy calculus", *Social Media + Society*, Vol. 3 No. 1, p. 2056305116688035, doi: 10.1177/2056305116688035.

Tucker, C.E. (2014), "Social networks, personalized advertising, and privacy controls", *Journal of Marketing Research*, Vol. 51 No. 5, pp. 546-562, doi: 10.1509/jmr.10.0355.

Tunggal, A.T. (2022), "The 65 biggest data breaches", available at: www.upguard.com/blog/biggest-data-breaches (accessed 4/2/2024).

van Ooijen, I., Segijn, C.M. and Opree, S.J. (2022), "Privacy cynicism and its role in privacy decision-making", *Communication Research*, Vol. 51 No. 2, p. 936502211060984, doi: 10.1177/00936502211060984.

Verduyn, P., Ybarra, O., Résibois, M., Jonides, J. and Kross, E. (2017), "Do social network sites enhance or undermine subjective wellbeing? A critical review", *Social Issues and Policy Review*, Vol. 11 No. 1, pp. 274-302, doi: 10.1111/sipr.12033.

Voss, K.E. (2023), "Composite-based and covariance-based structural equations modeling: moving forward by changing the dialogue", *European Journal of Marketing*, Vol. 57 No. 6, pp. 1780-1792.

Voukelatou, V., Gabrielli, L., Miliou, I., Cresci, S., Sharma, R., Tesconi, M. and Pappalardo, L. (2021), "Measuring objective and subjective wellbeing: dimensions and data sources", *International Journal of Data Science and Analytics*, Vol. 11 No. 4, pp. 279-309, doi: 10.1007/s41060-020-00224-2.

Webster, D., Dunne, L. and Hunter, R. (2021), "Association between social networks and subjective wellbeing in adolescents: a systematic review", *Youth and Society*, Vol. 53 No. 2, pp. 175-210, doi: 10.1177/0044118X20919589.

Whelan, E., Islam, A.K.M.N. and Brooks, S. (2020), "Applying the SOBC paradigm to explain how social media overload affects academic performance", *Computers and Education*, Vol. 143, p. 103692, doi: 10.1016/j.compedu.2019.103692.

Wisniewski, P., Xu, H., Lipford, H. and Bello-Ogunu, E. (2015), "Facebook apps and tagging: the trade-off between personal privacy and engaging with friends", *Journal of the Association for Information Science and Technology*, Vol. 66 No. 9, pp. 1883-1896, doi: 10.1002/asi.23299.

Wottrich, V.M., van Reijmersdal, E.A. and Smit, E.G. (2019), "App users unwittingly in the spotlight: a model of privacy protection in mobile apps", *Journal of Consumer Affairs*, Vol. 53 No. 3, pp. 1056-1083, doi: 10.1111/joca.12218.

Yang, H.C. (2013), "Young Chinese consumers' social media use, online privacy concerns, and behavioral intents of privacy protection", *International Journal of China Marketing*, Vol. 14 No. 1, pp. 82-101.

Yao, M.Z., Rice, R.E. and Wallis, K. (2007), "Predicting user concerns about online privacy", *Journal of the American Society for Information Science and Technology*, Vol. 58 No. 5, pp. 710-722.

Young, A.L. and Quan-Haase, A. (2013), "Privacy protection strategies on Facebook", *Information, Communication and Society*, Vol. 16 No. 4, pp. 479-500, doi: 10.1080/1369118X.2013.777757.

Zhang, R. (2017), "The stress-buffering effect of self-disclosure on Facebook: an examination of stressful life events, social support, and mental health among college students", *Computers in Human Behavior*, Vol. 75, pp. 527-537, doi: 10.1016/j.chb.2017.05.043.

Zhu, M., Wu, C., Huang, S., Zheng, K., Young, S.D., Yan, X. and Yuan, Q. (2021), "Privacy paradox in mHealth applications: an integrated elaboration likelihood model incorporating privacy calculus and privacy fatigue", *Telematics and Informatics*, Vol. 61, p. 101601, doi: 10.1016/j.tele.2021.101601.

Further reading

Bollen, K.A. (1989), "A new incremental fit index for general structural equation models", *Sociological Methods and Research*, Vol. 17 No. 3, pp. 303-316.

Graham, M.H. (2003), "Confronting multicollinearity in ecological multiple regression", *Ecology*, Vol. 84 No. 11, pp. 2809-2815.

Corresponding author

Park Thaichon can be contacted at: p.thaichon@gmail.com