January 2020

Managing consumer privacy concerns and defensive behaviours in the digital marketplace

Ruwan Bandara
University of Wollongong

Mario Fernando
University of Wollongong, mariof@uow.edu.au

Shahriar Akter
University of Wollongong, sakter@uow.edu.au

Managing consumer privacy concerns and defensive behaviours in the digital marketplace

Abstract

Purpose: The aim of this study is to examine privacy issues in the e-commerce context from a power-responsibility equilibrium theory (PRE) perspective. Design/Methodology/Approach: Data was collected using an online survey (n=335) from online shopping consumers. This study employed partial least squares-structural equation modeling (PLS-SEM) and fuzzy-set qualitative comparative analysis (fsQCA) techniques to empirically examine the proposed relationships. Findings: Lack of corporate privacy responsibility and regulatory protection can deprive consumers of privacy empowerment and damage consumer trust to trigger privacy concerns and subsequent defensive responses. Also, the fsQCA revealed five causal configurations to explain high consumer defensive behaviours. Research limitations/ implications: This study identifies the importance of PRE theory in the privacy context. Consumer privacy concerns, privacy empowerment, and trust are established as strong mediators between corporate/ regulatory privacy protection efforts and consumer backlash. The application of fsQCA verified that consumer privacy behaviour can be better explained by different configurations of the same causal antecedents. Practical implications: The findings highlight the importance of increasing trust and privacy empowerment as mechanisms to manage privacy concerns and consumer backlash through responsible organisational and regulatory privacy protections. The importance of balancing power and responsibility dynamics for maintaining a healthy information exchange environment is identified. Originality/value: This study extends the PRE framework of privacy to include corporate privacy responsibility, privacy empowerment, and trust. This is one of the first studies to explore both antecedents and outcomes of privacy empowerment. Also, the application of complexity theory and fsQCA to explain consumers' defensive responses is novel to the literature.

Publication Details

Bandara, R., Fernando, M. & Akter, S. (2020). Managing consumer privacy concerns and defensive behaviours in the digital marketplace. European Journal of Marketing, Online First 1-10.

Managing Consumer Privacy Concerns and Defensive Behaviours in the Digital Marketplace

Abstract

Purpose: The aim of this study is to examine privacy issues in the e-commerce context from a power-responsibility equilibrium theory (PRE) perspective.

Design/Methodology/Approach: Data was collected using an online survey (n=335) from online shopping consumers. This study employed partial least squares-structural equation modeling (PLS-SEM) and fuzzy-set qualitative comparative analysis (fsQCA) techniques to empirically examine the proposed relationships.

Findings: Lack of corporate privacy responsibility and regulatory protection can deprive consumers of privacy empowerment and damage consumer trust to trigger privacy concerns and subsequent defensive responses. Also, the fsQCA revealed five causal configurations to explain high consumer defensive behaviours.

Research limitations/implications: This study identifies the importance of PRE theory in the privacy context. Consumer privacy concerns, privacy empowerment, and trust are established as strong mediators between corporate/regulatory privacy protection efforts and consumer backlash. The application of fsQCA verified that consumer privacy behaviour can be better explained by different configurations of the same causal antecedents.

Practical implications: The findings highlight the importance of increasing trust and privacy empowerment as mechanisms to manage privacy concerns and consumer backlash through responsible organisational and regulatory privacy protections. The importance of balancing power and responsibility dynamics for maintaining a healthy information exchange environment is identified.

Originality/value: This study extends the PRE framework of privacy to include corporate privacy responsibility, privacy empowerment, and trust. This is one of the first studies to explore both antecedents and outcomes of privacy empowerment. Also, the application of complexity theory and fsQCA to explain consumers' defensive responses is novel to the literature.

Keywords Online privacy, Privacy empowerment, Power-responsibility equilibrium, Trust, Corporate privacy responsibility, Regulations, Complexity theory, fsQCA

Paper type Research Paper

Acknowledgments

Conflict of interest: None

Introduction

Consumer data induces extensive advantages and risks for both consumers and companies. In today's digital economy, the data generated by consumers has become a major marketing asset and a key revenue generator for companies. Inasmuch as that consumers' information creates revenue and provides a competitive advantage to companies, managing privacy issues has become a key impediment for marketing and a formidable barrier to e-commerce growth (Bandara et al., 2019; Ferrell, 2017; Holtrop et al., 2017; Martin and Murphy, 2017; Petrescu and Krishen, 2018).

Corporations hold asymmetric power over consumer data, and they have an inherent responsibility to properly manage data and protect consumer privacy (Flyverbom et al., 2019; Lwin et al., 2007; Zwitter, 2014). However, corporate data management efforts have created an unhealthy market environment with lack of trust and increased consumer vulnerability (Bandara et al., 2020a; Liao et al., 2011; Martin et al., 2017; Morey et al., 2015). Therefore, some scholars highlight the role of regulatory mechanisms to balance corporate power and achieve a healthy interaction level should be greater (Kucuk, 2016; Lwin et al., 2007). As asserted by Flyverbom et al. (2019, p. 15), "the roles and responsibilities of public and private actors when it comes to developing, operating, and governing digital infrastructures and the resources they command deserve much more scholarly attention." Given these developments, the power and responsibility dynamics surrounding online privacy and how they impact consumers, need to be better understood.

Consumers grow increasingly worried about their privacy and respond resentfully as the potential harm from firms collecting their data continues to expand exponentially. For instance, Martin et al. (2017) show that customer data vulnerabilities (e.g., data breach vulnerability, spillover vulnerabilities) lead to emotional and cognitive violations pushing consumers to act defensively by falsifying their information or switching their online behaviours. Likewise,

Poddar et al. (2009) also found that consumers' engagement in the online space can vary from compliance to blatant falsification of their information based on perceived fair play by firms, the criticality of the exchange, and felt invasion of privacy. Lwin et al. (2016) reveal that, due to low communication quality of firms and high sensitivity of the information being shared, consumers are now more worried about their privacy and they respond by taking deflective and defensive behaviours. Echoing the findings of these studies, we identify the necessity to inquire and advance knowledge regarding consumer privacy protection (Bandara et al., 2020b; Kannan, 2017; Martin and Murphy, 2017; Pappas, 2018). This is vital as "privacy research should be grounded in existing knowledge and needs a refocus to address this rapidly changing digital environment" (Ferrell 2017, p. 160).

In this study, we aim to understand what constitutes consumers' privacy concerns and behaviours in the digital marketplace from a power-relations perspective. For this purpose, we use the power-responsibility equilibrium (PRE) theory (Davis et al., 1980; Laczniak and Murphy, 1993; Murphy et al., 2005) and the PRE framework of privacy (Lwin et al., 2007). We specifically aim to answer (1) what are the impacts of power holders (i.e., corporate privacy responsibility and privacy regulations) on consumer privacy concerns, privacy empowerment and trust, and (2) what are the impacts of privacy concerns, privacy empowerment and trust on consumers' power-balancing strategies (i.e., defensive behaviours). Apart from identifying the direct causal antecedents, we also aim to identify different configurations or interactions of these antecedents to predict consumers' defensive behaviours. Hence, the study aims to answer (3) what configurations of privacy-related antecedents lead to consumers' highly defensive behaviours.

The findings of this study are significant for several reasons. First, the study highlights the significance of PRE theory in the consumer privacy context. PRE has been identified as a useful ethical and social responsibility approach to investigate consumer privacy issues

(Krishen et al., 2017; Martin and Murphy, 2017). However, its empirical application in the privacy context remains largely limited (i.e., Krishen et al., 2017; Lwin et al., 2007). By using PRE, the study provides an integrated view of consumer privacy in today's digital marketplace by amalgamating both antecedents and outcomes of privacy concerns and also by integrating consumer-business and citizen-government relationships within the same framework. Second, this study extends the PRE framework of privacy (Lwin et al., 2007) by including three new constructs: corporate privacy responsibility, privacy empowerment, and trust. Third, the study highlights the importance of increasing trust and privacy empowerment as mechanisms to alleviate privacy concerns and consumer backlash through organisational and regulatory efforts. Finally, this is one of the first studies to identify multiple causal configurations to predict consumers' privacy-related defensive behaviours based on complexity theory (Fiss, 2011; Woodside, 2014) and fuzzy-set qualitative comparative analysis (fsQCA) (Ragin, 2008).

The following sections of the paper discuss the theoretical basis of the study, methods used to empirically test the proposed model, and the findings of the study. This will be followed by a discussion on the results and potential contributions of the study.

Theoretical background

Power-responsibility equilibrium

The power-responsibility equilibrium theory advocates the balance between social power and social responsibility (Davis et al., 1980; Laczniak and Murphy, 1993; Murphy et al., 2005). In a balanced-power relationship, "people should treat others as equals, be more concerned about the welfare of others, and give benefits to others non-contingently" (Schaerer et al., 2018, p. 78). Accordingly, this theory suggests that the powerful member in a relationship should exhibit power and responsibility equally toward the less powerful member. Those who do not

use power in a way that society considers responsible will lose their power in the long run (Caudill and Murphy, 2000).

Based on the power-responsibility equilibrium theory, Lwin et al. (2007) developed the PRE framework of privacy. The authors clarified corporations and government on one side – the power holders who are expected to show responsibility and on the other side of consumers – the information providers who expect responsible use of power. Accordingly, consumers will take defensive actions when corporations and governments fail to promote equality in information exchange and effectively manage privacy protection. These defensive actions are driven by deficits in privacy protection by power holders (Caudill and Murphy, 2000; Lwin et al., 2007). The PRE framework of privacy is important as it integrates consumer-business and citizen-government relationships and thereby illustrates a broader integrated view of the influence of power holder responsibility on potentially damaging consumer actions. It is also useful as it imparts an integrated systems view by modelling privacy concerns of consumers as a mediating variable, indicating both of its causal and consequential roles.

This study introduces an extended PRE framework of privacy (see Figure 1). We initiated this study with an extensive literature review, which was followed by a qualitative study based on semi-structured interviews with 30 online shopping consumers. We identified four themes related to consumers' online privacy concerns, including corporate privacy responsibility, regulatory protection, consumer trust, and consumer privacy empowerment. These findings were incorporated into the PRE framework of privacy (Lwin et al., 2007). The focus of this paper is to empirically examine the proposed relationships indicated in Figure 1 using survey data.

Insert Figure 1 here

Consumer privacy concerns

Information privacy is germane to the flow of information—what, by whom, why, and how information is collected and used (Bandara et al., 2019; Martin, 2016b). The study maintains that privacy concerns reflect worries when information is collected and used by entities for purposes and in ways that were not intended by the individual (Bandara et al., 2019). Consumers' privacy concerns have risen due to the extensive amount and diverse methods of data collection. With the proliferation of big data, large volumes and varieties of data are seamlessly available to several parties to be readily exploited with relatively cheap yet advanced tools (Martin, 2016a; Martin et al., 2017). The apparatus that collect and generate large volumes and varieties of data are mostly invisible to consumers: The collection of data does not merely depend on direct interactions anymore (King and Forder, 2016). The secondary uses of data and third parties having access to consumer data have increased. Companies increasingly share data with tracking firms. They also sell to data aggregators. These data aggregators consolidate data from different sources and re-sell data in the market (Flyverbom et al., 2019). Such practices have raised privacy concerns as the obfuscation of data has made it impossible for consumers to trace which information, how and from what sources their data is collected (West, 2019).

Concerns over consumer profiling are also increasing. Companies develop extensive profiles of consumers from gathered and discovered data (King and Forder, 2016). Consumers hardly have access to these profiles. Decisions are increasingly being made about consumers based on these profiles, yet these profiles carry inaccurate and erroneous information. Moreover, the use of discovered data and tools such as data analytics enable companies to reveal de-identified data including sensitive personal data that a consumer may not prefer to share or be profiled (Kshetri, 2014). In this study 'privacy concerns' construct is theorised as a

unidimensional construct reflecting above concerns about privacy (Lwin et al., 2016; Miltgen et al., 2016; Mousavizadeh et al., 2016).

Privacy empowerment

The importance of consumer power, control, and empowerment on the internet has been discussed over the years (Kucuk, 2016). A few scholars have also focused on exploring information privacy empowerment. However, most definitions maintain that privacy empowerment is essentially commensurate with someone having control over their information. For instance, privacy empowerment is identified as "a psychological construct related to the individual's perception of the extent to which they can control the distribution and use of their personally identifying information" (van Dyke et al., 2007, p. 71). At a broader level, privacy empowerment can be clarified as consumer beliefs that they can produce desired outcomes and prevent undesired outcomes related to the use of their information (Bandara et al., 2020b). Accordingly, having control can be considered as a necessary but not adequate condition to reflect privacy empowerment.

According to the psychological empowerment theory (Spreitzer, 1995; Zimmerman, 1995), empowerment is reflected in outcomes and cognitions such as control, critical awareness, self-determination, competence, and self-efficacy (Perkins and Zimmerman, 1995; Spreitzer, 1995). By having control, one can exert influence over decisions that matter to one (Malhotra et al., 2004). Self-determination or autonomy reflects the choices individuals have over initiating and regulating their actions (Thomas and Velthouse, 1990). Critical awareness, as an integral part of empowerment enables individuals to understand the resources available to achieve goals and norms and values of the environment around them (Zimmerman, 1995). Self-efficacy is another key aspect of empowerment which shows an "individual's belief in his or her capability to perform activities with skill" (Spreitzer, 1995, p. 1443).

We concur with Kucuk (2009, p. 327) that, "although consumer sophistication and empowerment are on the rise as a result of the digital revolution, there is insufficient academic exploration with the aim of understanding how this empowerment functions on the internet." This is particularly true when it comes to privacy empowerment research. We also maintain that "empowerment has been identified as a growing force in marketing […]. As its prevalence increases, the need to understand its antecedents and consequences also increases" (Hunter & Garnefeld, 2008, p. 2).

Consumer trust

Despite the growth of e-commerce over the years, lack of trust remains a fundamental challenge (Arli et al., 2018; Bandara et al., 2020a; Pappas, 2018). This is understandable, considering the reverberations of technological transformations surrounding online shopping, such as the use of big data analytics and massive data aggregation. Trust is assured when consumers perceive favourable conditions exist to enable successful transactions (McKnight and Chervany, 2001; Mou et al., 2017).

Trust is defined as "a psychological state comprising of the intention to accept vulnerability based on positive expectations from the intentions or behaviours of another" (Rousseau et al., 1998, p. 395). Developing trust is an ongoing, dynamic process that matures with regular interactions. Trust reflects consumers' overall perception on their willingness to depend on online sellers' benevolence, integrity, competence and predictability, and dependability of the enabling technological environment (i.e., the internet) to meet their privacy expectations (Akter et al., 2011; McKnight et al., 2002; Mou et al., 2017). Based on previous research (e.g., Dinev and Hart, 2006; Lwin et al., 2016; Malhotra et al., 2004), we measure these perceptions operationalising trust as a unidimensional construct.

Several scholars have considered trust as an important factor in investigating privacy. However, according to Miltgen and Smith (2015, p. 743) "its specific relationship with other privacy-related constructs has not been consistently examined across studies, with trust serving as an antecedent, outcome, mediator, or moderator." Also, trust has been studied mostly as an antecedent of promotion-focused behaviours, but there are few empirical studies on the relationship between trust and prevention-focused privacy behaviours. Moreover, literature shows that "as customers develop both trust and privacy beliefs […] these aspects [should] be studied together to fully comprehend possible combinations between them, capable of explaining their behaviour" (Pappas, 2018, p. 1683).

Corporate privacy responsibility

As identified by PRE framework of privacy and other studies (e.g., Pollach, 2011), corporations have an intrinsic responsibility to their customers, particularly due to the size and asymmetric power they hold over data. The perceived corporate privacy responsibility in this study reflects consumer perceptions of corporate obligations to consumer privacy protection. Most of the studies, including the PRE framework of privacy, focus on consumer perceptions of the *privacy policy* to conceptualise or measure how corporations exercise power and responsibility (Lwin et al., 2007; Wu et al., 2012).

Consumer expectations of corporate privacy obligations are diverse. As explained in the procedural justice literature, privacy policy and notices are key procedures that reflect a firm's initiative to protect consumer privacy (Culnan and Armstrong, 1999). The shortcomings of privacy notices can lead to consumer concerns over privacy as well as a detrimental effect on trust (Bandara et al., 2020a; Petrescu and Krishen, 2018). Hence, providing clear and understandable terms of how consumer information is collected and used, is a primary

responsibility that highlights the importance of providing notice and obtaining informed consent. A key barrier to taking informed privacy decisions is due to the lack of awareness of how data is being collected and used (Awad and Krishnan, 2006). This is mainly due to information asymmetries and lack of transparency (Petrescu and Krishen, 2018; West, 2019). Transparency is considered a key determinant to ensuring trust in the online environment (Arli et al., 2018). It can also diminish privacy concerns (Krishen et al., 2017). Consumer privacy concerns are heavily influenced by fairness judgements. Consumers share their information and risk their privacy for expected benefits. Therefore, information exchanges are not inherently value-free; they carry expectations that companies will use information fairly for given purposes and provide value in exchange for their information (Culnan and Bies, 2003; Krishen et al., 2017). Violation of privacy has emerged as one of the most critical ethical issues in the data-driven marketplace (Bandara et al., 2020a; Martin, 2016a; Zwitter, 2014). Consumers divulge their information with the expectation that organisations will maintain minimal ethical standards of information use. Hence, corporations need to incorporate not only legal but ethical responsibilities to their data privacy management practices (Ferrell, 2017).

Regulatory protection

Regulatory protection refers to how various government and industry agencies devise internet privacy regulations to direct and police the use of consumer data (Lwin et al., 2007). Regulation plays a vital role in reaching market equalisation to balance corporate power and empower consumers to achieve a healthy interaction level (Kucuk, 2009). With the rapidly changing technological environment, consumers are limited in their knowledge of dealing with online privacy and security issues and rely upon laws and institutional safety mechanisms for protection (Kim and Kim, 2011; Lwin et al., 2007). Apart from the government regulatory protection, third-party watchdogs, which are usually formed by industry groups or certifying

agencies (e.g., TRUSTe and Direct Marketing Association), work to substitute for and to complement government regulations. These regulatory bodies issue certificates or seals assuring that online firms have adhered to information practices they have agreed to act upon (Kim et al., 2008b; Lwin et al., 2007).

Exploring the impact of regulatory protection is important as "no treatment of privacy will be complete without explicit recognition of the role of government" (Stewart, 2017, p. 158) or other regulators for that matter. Researchers also identify the role of regulation in dealing with systematic consumer vulnerabilities as well as improving consumer empowerment. To date, no study has investigated the impact of regulatory protection on consumer privacy empowerment. The PRE framework of privacy argues that power holders are expected to ensure a trusting environment for consumer privacy protection. However, there is a paucity of empirical research exploring the impact of regulation on establishing trust and its effect on consumer privacy and behaviour (Miltgen and Smith, 2015).

Research hypotheses

Impact of privacy concerns on behaviour

According to the PRE framework of privacy, consumers balance perceived deficits in privacy protection by power holders with defensive actions. Individuals respond using different strategies to overcome vulnerabilities created as a result of power holder practices. This may include protective behaviours, using tools and privacy-enhancing technologies such as virtual private networks, software to eliminate cookies and pop-ups, private browsing and using identity anonymisers (Lwin et al., 2016). The fabrication of information is another defensive mechanism that involves misrepresenting or disguising one's identity by using fictitious and false information (Wirtz et al., 2007). In the online shopping context, fabrication can often occur when companies request too much information beyond the transaction purpose. When

consumers perceive companies are overpowering or if they want to avoid the risk of information misuse, they tend to withhold their information or withdraw from the relationship. Consumers tend to refuse to share information when the perceived threat level is high (Choi et al., 2018; Lee et al., 2013). Withholding or refusing to provide information might restrain a consumer from processing transactions. Therefore, it can be costly in one way but also very effective in responding to power imbalances in the marketplace. In summary, the study argues that privacy concerns will influence consumers to take defensive actions. Thus the study hypothesises that:

H1: Privacy concerns have a significant positive effect on defensive behaviours.

Impact of privacy empowerment

In today's big data environment, consumers can find it challenging to reach desired goals or avoid undesired outcomes in terms of their privacy. For instance, the lack of control over information can engender a sense of risk of losing their information and perceptions of being invaded (Culnan and Armstrong, 1999; Wang et al., 2016). Companies often provide only limited control to consumers (e.g. temporary opt-out), but research shows that having more control can lessen individuals' privacy concerns (Choi et al., 2018; Dinev and Hart, 2004). Lack of autonomy over the choices of data has encouraged consumers to feel powerless to manage or determine the uses of their own personal information (Kim and Kim, 2011). According to some critics, choice of privacy is just an illusion – consumers lack real opt-in and opt-out options, and thereby consumers are increasingly worried about their privacy. Similarly, lack of competence and efficacy can result in lack of privacy empowerment and thereby increase consumers' privacy concerns (Akhter, 2014). Therefore, similar to Kim and Kim (2011) and van Dyke et al. (2007), we argue that privacy empowerment will have a negative effect on privacy concerns. Privacy studies are yet to reveal the impact of privacy

empowerment on defensive behaviours. This study proposes a negative relationship between privacy empowerment and defensive behaviours. For instance, a person having control will barely have the need to falsify their information or to avoid using online services (Yun et al., 2018). Similarly, consumers with privacy efficacy have a tendency to conduct online transactions rather than withdrawing from online behaviours (Akhter, 2014). Hence the study hypothesises that:

H2a: Privacy empowerment has a significant negative effect on privacy concerns

H2b: Privacy empowerment has a significant negative effect on defensive behaviours

Impact of Trust

Consumer trust is one of the most widely researched topics in privacy research. Some studies have found trust as a solution to lessen risk perceptions – trust lowers perceived risk (Kim et al., 2008a; Taylor et al., 2009) and other studies show that lower level of risk perceptions form a high level of trust (van Dyke et al., 2007). This study focuses on the former, and argues that in an environment where trust is established, consumers will develop lower privacy concerns. For instance, when consumers perceive that online sellers have the ability to deal with data breaches and the unauthorised secondary use of data, they will have lower privacy concerns. This direction of the trust-risk relationship is appropriate for the study as the focus is on what contributes to consumer privacy concerns and how consumers respond. Trust is widely researched as a significant positive determinant of several promotion-focused consumer intentions and behaviours, including purchasing (Kim et al., 2008a; Liao et al., 2011) and relationship building (Wirtz and Lwin, 2009). However, there is a paucity of research on the relationship between trust and prevention-focused behaviours such as defensive behaviours. As mentioned earlier, trust prompts consumers to accept vulnerability based on positive expectations about online sellers' privacy practices. Hence, it can be assumed that consumers

will take fewer defensive actions in such conditions. However, when they perceive high vulnerability due to opportunistic behaviour of sellers, they will resort to defensive behaviours. For instance, consumers avoid the risk of information misuse by deciding not to disclose information (Choi et al., 2018) and trust guarantees that consumers are unperturbed in directly disclosing their information (Mou et al., 2017). Hence, the study hypothesises that:

H3a: Trust has a significant negative effect on privacy concerns

H3b: Trust has a significant negative effect on defensive behaviours

Impact of corporate privacy responsibility

According to PRE theory, the more powerful partner in a social exchange is required to show corresponding levels of responsibility to establish trust and thereby reduce consumer privacy concerns (Caudill and Murphy, 2000; Lwin et al., 2007). As explained by the social contract view of privacy, exchange of information is governed by norms and contracts (Culnan and Bies, 2003; Martin, 2016b). Any violation of such contract, whether it be legal or hypothetical, involves a psychological contract breach that can result in adverse emotional and affective states such as loss of trust (Morrison and Robinson, 1997). Corporate privacy practices should also lead to increased consumer control over their own data and enable them to be aware of and to decide as to how their information should be used. For instance, greater transparency will increase consumers' critical awareness of the sellers' data usage and privacy practices. Hence, it can be argued that responsible data practices can ensure consumers feel empowered as they will have better awareness, ability to protect themselves, and also choices that assure safe information sharing (Kucuk, 2016; Martin and Murphy, 2017). Therefore, the study hypothesises that:

H4a: Corporate privacy responsibility has a significant positive effect on trust.

H4b: Corporate privacy responsibility has a significant negative effect on privacy concerns.

H4c: Corporate privacy responsibility has a significant positive effect on privacy empowerment.

Impact of regulatory protection

Consumer perceptions of regulatory protection stimulated by legislative and third-party privacy safeguarding mechanisms are considered significant determinants of consumer privacy concerns (Kim and Kim, 2011; Lwin et al., 2007). Hence, consumers' positive perceptions about regulatory protection will lessen their level of privacy concerns. Also, it will ensure a trusting exchange environment where consumers will willingly share their information and conduct transactions. As identified in the consumerism literature, stringent government laws and effective industry regulations will enhance consumer empowerment (Kucuk, 2009; Kucuk, 2016). Regulations have been found to increase consumers' ability to control their information, ability to protect their privacy, and also ensure more choices regarding their information use (Kim et al., 2008b; Lwin et al., 2007). Therefore, it can be argued that consumers' positive perceptions regarding regulatory protection will increase the perceived level of privacy empowerment. Hence, the study hypothesises that:

H5a: Regulatory protection has a significant positive effect on trust.

H5b: Regulatory protection has a significant negative effect on privacy concerns.

H5c: Regulatory protection has a significant positive effect on privacy empowerment.

Complexity theory and research proposition

Complexity theory is highly useful in understanding the complex nature of human behaviours. This theory asserts that multiple combinations of factors or multiple paths (i.e., configurations) could lead to the same outcome (Fiss, 2011; Woodside, 2014). Also, the same condition of a factor when combined with different conditions of other factors could lead to different outcomes. Complexity theory is based on the principle of equifinality that asserts "outcome of interest can equally be explained by alternative sets of causal conditions that combine in sufficient configurations for the outcome" (Pappas et al., 2016, p. 796).

This configurational approach relies on combinations of a set of causal conditions to capture complex interaction effects rather than focusing on independent causal conditions to explain or predict a certain outcome. Therefore, apart from the individual causal conditions identified in previous hypotheses, we also focus on the configurations of these causal conditions to predict the ultimate outcome variable (i.e., defensive behaviours). Hence, we present the following proposition:

Proposition 1: No single best configuration of factors leads to a high level of privacy-related defensive behaviours, but there exist multiple, equally effective configurations of causal factors.

Methods

Study design and sampling

This study focuses on privacy issues in the digital marketplace. Specifically, we focus on business to consumer (B2C) e-commerce context. The investigation of privacy issues in this context continues to be a critical issue due to evolving technologies that encourage the vast collection and myriad uses of consumer data (Bandara et al., 2019; Martin and Murphy, 2017). We collected data using an online survey. The participants were online shopping consumers in

Australia. They were selected based on whether they had shopped online during the last three months in Australia.

The measurement items were adapted from different contexts from prior literature to develop the online survey questionnaire. Few items were developed based on either the literature or interview data. In order to ensure the validity of the survey questionnaire, a systematic scale validation procedure was followed (MacKenzie et al., 2011). The constructs and their measurement items are indicated in Appendix A. All constructs were measured using a 7-point Likert scale (e.g., strongly disagree – strongly agree). The model controls for several factors, including demographic variables, internet experience, online shopping frequency, previous privacy experience, and information sensitivity. The survey was pretested with 21 respondents, including subject experts and online consumers. Next, a pilot test was conducted with 75 online shopping consumers. The final online survey was managed by a leading market research company. Random sampling was used to obtain survey responses. Two attention check questions (ACQs) were used in the survey to ensure response quality (Peer et al., 2014). This helped to screen out inattentive respondents – a major limitation in online surveys. Apart from that, flatlines and speeders were checked and eliminated manually. Finally, 335 valid responses were included in the final analysis. The demographic profile of the sample is indicated in Table 1.

Insert Table 1 here

Data analysis

This study employed mainly two data analysis techniques, namely, partial least squares-structural equation modelling (PLS-SEM) and fsQCA. PLS-SEM was employed to examine the direct and mediating relationships among the observed variables. SEM is a second-generation multivariate analysis technique which can simultaneously analyse relationships among multiple independent and dependent variables (Hair Jr et al., 2019a). PLS-SEM is usable for exploratory research and has a primary focus on prediction (Hair Jr et al., 2017; Hair Jr et al., 2019a; Hair Jr et al., 2019b). Thereby, it suits the objective of this study well. Further, PLS-SEM can deal with large and small sample sizes and is suitable for non-normal data as well. The proposed model of the study is reflective as the causality goes from constructs to items (Akter et al., 2017). Apart from the hypotheses testing, the study conducted a mediation analysis to generate additional insights. This study used nonparametric bootstrapping with 5000 sub-samples to obtain the estimations (Hair Jr et al., 2017).

This study also employed fsQCA, which moves beyond traditional symmetric techniques that rely on linear causality and the net effects of a set of antecedents on outcomes, to analyse combined and interactive effects of antecedents on outcomes (Woodside, 2013). By using fsQCA, we aim to identify complex causations by exploring interdependencies among several antecedent factors and their impact on consumers' privacy-related defensive behaviours. Such an endeavour was not possible with the PLS-SEM technique. Based on equifinality principle, we identify different configurations that can lead to the outcome (i.e., defensive behaviours). Also, using fsQCA, the study distinguishes variables that are present to cause a certain outcome from variables that are absent to cause the same outcome (Ragin, 2008). The use of both approaches in the study enables us to understand not only the unidirectional effects but also alternative causal pathways to explain the outcome, and thereby provide a more holistic representation of the investigated model.

The study conducted data analyses using SmartPLS 3.2 (Hair Jr et al., 2017), SPSS 25.0 and fsQCA 3.1b (Ragin, 2018) computer software.

Results

PLS-SEM analysis and results

Assessment of the measurement model

The measurement model was evaluated based on composite reliability (CR), convergent validity, and discriminant validity. The outer loadings of all the constructs were greater than the acceptable level of 0.7, ranging from 0.706 to 0.853 at significance level P<.001, indicating a strong association with respective constructs (Hair Jr et al., 2017). The internal consistency reliability measured using composite reliability (CR) was above the recommended value of 0.7 for all constructs. Similarly, convergent validity was confirmed as average variance extracted (AVE) values were above the recommended value of 0.5. The outer loadings, CR and AVE values of each construct are indicated in Table 2. The discriminant validity of the model was tested by examining the correlation matrix (Fornell-Larcker criteria). The square root of AVE for all the constructs was higher than the inter-construct correlations (Fornell and Larcker, 1981) and hence discriminant validity was established. However, recent studies recommend using Heterotrait-Monotrait ratio of correlations (HTMT) as a more robust measure of discriminant validity (Hair Jr et al., 2019b). The HTMT statistic should not exceed 0.90 (Hair Jr et al., 2019b) and all the constructs in the study were below this threshold. The correlation matrix and HTMT results are indicated in Appendix B and Appendix C, respectively. Overall, the evaluation of the measurement model justifies the utilisation of all the constructs in the hypothesised model.

Insert Table 2 here

Assessment of the structural model: Hypotheses testing

The structural model was estimated using the bias-corrected and accelerated bootstrapping procedure with 5000 resamples. Table 3 presents the results of the path coefficients of the structural model. All of the path coefficients were significant at the p-value of < 0.001 except for REG_PROT and PRV_CON, which was significant at the p-value of < 0.01. Hence, all the hypotheses of the study were supported. The inclusion of the control variables (age, gender, internet experience, privacy experience, shopping frequency, and information sensitivity) did not show a significant effect.

Insert Table 3 here

The study analysed R^2 values to identify the amount of variance in the endogenous construct explained by the exogenous construct(s). The proposed model accounted for 55.2% of the variance in DEF_BEH (R^2 = 0.552, t = 15.897). Moreover, the model explained 62.8% variance in PRV_CON (R^2 = 0.628, t = 19.673), 56.7% variance in TRST (R^2 = 0.567, t = 15.724), and 48.9% variance in PRV_EMP (R^2 = 0.489, t = 13.220). The findings of the structural model are presented in Figure 2.

Further, to evaluate the model's capability to predict, the blindfolding procedure was performed (with omission distance = 7) to obtain cross-validated redundancy measures based on Stone-Geisser's Q^2. The results showed Q^2 value for PRV_CON (0.366), TRST (0.347), PRV_EMP (0.259), and DEF_BEH (0.300), which are greater than zero, indicating acceptable predictive relevance (Hair Jr et al., 2019a; Hair Jr et al., 2019b).

We also checked for the out-of-sample predictive power of the ultimate outcome variable based on PLSpredict. As recommended by Shmueli et al. (2019), we conducted PLSpredict with 10 folds and 10 repetitions. All the indicators of defensive behaviour construct showed a lower root mean squared error (RMSE) values in PLS-SEM compared to RMSE values of the linear regression model (LM) benchmark, confirming that the model has high predictive power (Shmueli et al., 2019).

Insert Figure 2 here

Mediation analysis

The study conducted mediation analysis to generate additional insights. Mediation was conducted by following the guidelines of Hayes (2017) and Preacher and Hayes (2008). Hence, both direct and indirect effects were considered. The direct effects were identified previously (Table 3) and indirect and total effects between constructs are mentioned in Table 4. The study found that CP_RES has both direct (β = -0.194, t = 3.625) and indirect (β = -0.237, t = 6.127) effect on PRV_CON. Thereby, TRST and PRV_EMP can be considered as partial mediators between CP_RES and PRV_CON. Similarly, REG_PROT showed both direct (β = -0.151, t = 2.802) and indirect (β = -0.204, t = 5.859) effect on PRV_CON. Hence, TRST and PRV_EMP were found to partially mediate the relationship between REG_PROT and PRV_CON. It was also found PRV_CON as a partial mediator between TRST and DEF_BEH. TRST showed direct (β = -0.255, t = 4.520) as well as indirect effect (β = -0.080, t = 3.163) on DEF_BEH. Further, PRV_CON was also found as a partial mediator between PRV_EMP and DEF_BEH. PRV_EMP showed a significant direct effect (β = -0.254, t = 4.334) and indirect effect (β = -0.100, t = 3.564) on DEF_BEH. CP_RES was found to indirectly influence DEF_BEH (β = -0.352, t = 9.454). Hence, this relationship is partially mediated by TRST, PRV_CON, and

PRV_EMP. A similar effect was found between REG_PROT and DEF_BEH, as shown by its indirect effect (β = -0.300, t = 8.218).

Insert Table 4 here

fsQCA analysis and results

The first step of fsQCA involved calibration of crisp values of data into the fuzzy form. In other words, the seven-point Likert scale data was transformed into fuzzy set scores ranging from full membership to full non-membership. In the study, 6 was considered as the full membership, 2 as full non-membership, and 4 as the cross-over point (Pappas, 2018). Gender was measured based on two categories. Therefore, indirect calibration was used (male = 1, female = 0) (Fiss, 2011, Ragin, 2018).

Next, we examined whether any causal conditions were *necessary* to explain the outcome. A causal condition is considered necessary if it is needed for an outcome to occur (Ragin, 2008) and the corresponding consistency score of a particular causal condition should exceed the threshold of 0.90 (Pappas, 2018). As Table 5 suggests, of the 11 conditions considered, only privacy concerns and internet experience are necessary conditions for the consumers to take defensive actions and behaviours.

Next, a truth table containing all possible combinations of antecedent conditions of the outcome was produced. The truth table was then refined to produce the final solutions based on frequency and consistency (Ragin, 2008; Ragin, 2018). A frequency cut-off of one is preferred for smaller samples, but a higher cut-off is recommended for larger samples (e.g., above 150 or more samples) (Ragin, 2018). Hence, for this study, minimum observation frequency was set to two, and also a consistency cut-off value of 0.85 was considered (Pappas et al., 2016).

Next, based on the revised truth table, intermediate solutions that represent the most reasonable configurations to predict consumers' defensive behaviours were generated. The results generated five intermediate solutions, as indicated in Table 6. In fsQCA, results can be interpreted using two parameters, namely consistency and coverage. Consistency represents "the degree to which membership in each solution term is a subset of the outcome" (Ragin, 2018, p. 61). A consistency value over 0.8 indicates that the configuration(s) predict the outcome properly. Coverage measures the empirical relevance of a consistent subset (Ragin, 2008). The analysis also produces the solution coverage – the degree to which the outcome can be determined based on the set of configurations and is comparable to the R^2 value reported in correlational methods (Pappas, 2018). The intermediate solutions to predict consumers' defensive behaviours are presented in Table 6. Black circles (●) denote the presence of a condition, while crossed-out circles (⊗) indicate its negation. Blank spaces suggest a do not care situation, in which the causal condition may be either present or absent with no influence on the solution. In fsQCA, * represents "and" and ~ indicates "negation of condition".

Insert Table 5 here

Insert Table 6 here

According to the fsQCA results (Table 6), five different causal configurations of studied factors encourage consumers to take privacy-related defensive behaviours. The consistency of the five configurations is above the threshold value and can be considered adequate (consistency = 0.92). The overall solution coverage explains 64% of the outcome.

For consumers to show higher defensive behaviours, all five solutions reveal that consumers need to have higher privacy concerns (PrvCon) and internet experience (IntExp), combined with absence of privacy empowerment (~PrvEmp), corporate privacy responsibility

(~CPRes), regulatory protection (~RegPro), and trust (~TRST). In addition to the combination of these core constructs, the first solution identifies that higher defensive behaviours are reflected by females (~Gender) with lack of privacy experiences (~PrvExp) and consider the information they share is less sensitive (~InfSen). The second solution indicates that apart from the core constructs, consumers with lack of privacy experiences (~PrvExp) and perceived information sensitivity (~InfSen) but having higher shopping frequency (ShpFrq) will take higher defensive behaviours; the age and gender is not a matter according to this solution. The third solution identifies that apart from the core constructs, consumers who are older (Age) with lack of privacy experiences (~PrvExp) and perceived information sensitivity (~InfSen) will show more defensive behaviours. The fourth solution indicates that apart from the core constructs, consumers who are older (Age) with lack of privacy experiences (~PrvExp) and higher shopping frequency (ShpFrq) will show more defensive behaviours. The final solution recognises that apart from the core constructs, males (Gender) who are older (Age) with higher shopping frequency (ShpFrq) but with lack of perceived information sensitivity (~InfSen) will take higher defensive actions. Overall, the results support proposition 1 that there are multiple causal configurations to predict consumer behaviour.

We also tested for predictive validity using a subsample and a holdout sample (Pappas et al., 2016; Woodside, 2014). The magnitude of consistency and coverage values of the configurations are evidence of the predictive validity for predicting the causal model with another sample. The results indicated that coverage (subsample 1= 0.59, subsample 2= 0.60) and consistency (subsample 1= 0.92, subsample 2= 0.92) were not drastically different among the two sub-samples, indicating adequate predictive validity.

Additional analyses

The non-response bias between early and late respondents was tested using a t-test and no statistical differences were found (Tsou and Hsu, 2015). We followed guidelines of Kock (2015) and checked for CMB using the full collinearity test. All the VIF values were less than 3.3, confirming that the model is free from common method bias. In addition, following Podsakoff et al., (2003), the anonymity of the survey responses was assured, and it was clearly communicated that there are no right or wrong answers. This helped to minimise CMB that can inflate the relationships between exogenous and endogenous variables. Further, endogeneity bias was tested using Ramsey regression equation specification error test (Lai et al., 2018; Queiroz and Wamba, 2019). Endogeneity bias is indistinguishably linked with the recursivity of a structural model, mostly in cases of cross-sectional data (Lai et al., 2018). According to Queiroz and Wamba (2019, p. 75), endogeneity bias can occur as "cross-sectional data can result in a mis-specified model, because the variance in an exogenous variable can be endogenous to the model". The study did not find evidence of endogeneity bias in the data ($p > 0.05$).

Discussion and conclusions

Based on a power relations approach, we tried to explain consumers' privacy concerns and defensive behaviours when shopping online. PLS-SEM results indicated that corporate privacy responsibility ($\beta = -0.352$), regulatory protection ($\beta = -0.300$), trust ($\beta = -0.335$), and privacy empowerment ($\beta = -0.354$) negatively influence defensive behaviours while privacy concerns positively influence defensive behaviours ($\beta = 0.319$). Interestingly, all the five configurations in fsQCA results revealed similar effects – the presence of privacy concerns and absence of corporate privacy responsibility, regulatory protection, privacy empowerment and trust resulted in higher consumer defensive behaviours in all solutions (with a combination of other

factors such as internet experience). Therefore, the findings of both analysis methods complement each other to verify the proposed relationships. The mediation roles played by privacy concerns, trust, and privacy empowerment, indicate that power holders (firms and regulators) can manage consumer backlash by focusing on consumers' privacy issues, establishing a trusting and confident information exchange environment, and augmenting consumer privacy empowerment. Another interesting result relates to the influence of the internet experience of consumers. The fsQCA findings revealed that internet experience as a necessary condition for higher defensive actions. This finding is realistic as the more the consumers have experience using the internet, the more knowledge they will have about how to protect themselves by taking measures such as using VPNs, private browsing, or taking advanced measures to fabricate their information or to completely prevent companies collecting their data (Lwin et al., 2016; Youn, 2009).

Although PLS-SEM did not find any influence of control variables, including demographics factors such as age and gender and contextual factors such as perceived information sensitivity, fsQCA results revealed additional insights. For instance, females with higher internet experience tend to take more defensive actions (solution 1) and older males with higher internet experience tend to follow similar behaviours (solution 5). Overall, fsQCA models explain consumer defensive behaviours (64.1%) better than the PLS-SEM model (55.2% of variance). The fsQCA results also explain why some relationships we found contradict previous findings in the literature. For instance, higher information sensitivity (Lwin et al., 2007) and previous privacy violation experiences (Bandara et al., 2020b) generally lead to more defensive behaviours. Our results indicate that consumers will take higher defensive actions although the information is less sensitive and they have lack of previous privacy experiences (e.g., solution 1: PrvCon*~PrvEmp*~CPRes*~RegPro*~TRST*IntExp*~PrvExp*~InfSen*~Gen). The reason

is that there are other critical factors. According to solution one, these include higher privacy concerns combined with lack of privacy empowerment, corporate privacy responsibility, regulatory protection, trust, and internet experience that will influence consumers to act defensively.

Theoretical implications

The study findings have several theoretical implications. First, the study highlights the significance and applicability of PRE theory to elucidate privacy issues in the online context. By using PRE, this study fuses consumer-business and citizen-government relationships and illuminates the role of corporations and government on consumer privacy, trust and privacy empowerment within the same framework. By accomplishing this, the study extends the initial PRE privacy framework (Lwin et al., 2007) to include two new mediating variables. As privacy investigations that provide an integrated view are scanty in the marketing scholarship (Lwin et al., 2007; Martin and Murphy, 2017), these are significant contributions to theory.

Second, this study is among the few to comprehensively investigate consumer privacy empowerment. The study contributes immensely to theory, as this is one of the first studies to investigate both antecedents and outcomes i.e., the mediating effect of privacy empowerment, and thereby provides several new findings. The study uncovers that positive perceptions regarding corporate privacy responsibility and regulations effectuate privacy empowerment (i.e., the direct effect). It was also found on one hand that corporations and government can reduce privacy concerns of consumers by elevating privacy empowerment (i.e., the indirect effect). On the other hand, privacy empowerment reduces the number of consumers acting defensively (i.e., the direct effect). Also, privacy empowerment can reduce privacy concerns and thereby lessen consumers' defensive actions (i.e., the indirect effect). Our findings extend previously established privacy empowerment - privacy concerns relationship (Midha, 2012;

van Dyke et al., 2007) to explain their interactive effects in predicting consumer privacy behaviour.

Third, trust has been widely investigated in relation to consumer privacy in the online shopping context. However, there has been little attention paid to understanding the impact of power holder initiatives that enhance trust among consumers, especially of regulations (Miltgen and Smith, 2015). This study identifies the need for both responsible corporate privacy practices and effective regulatory mechanisms to strengthen trust perceptions and to minimise consumer privacy concerns, as well as power-balancing defensive responses. In addition, most trust studies focus on the impact of trust on promotion-focused behaviours. However, there is a paucity of literature concerning the relationship between trust and prevention-focused behaviours. The study findings confirm ensuring trust as a course of action to mitigate defensive consumer responses. The findings are also important, as scholars have highlighted the necessity of studies to inquire trust and privacy beliefs together, to accurately understand their combined effect on consumer behaviour (Pappas, 2018). Researchers can integrate our findings on power holder effects into existing models of trust (Kim et al., 2008a; Kim and Kim, 2011; Midha, 2012) to produce a much more comprehensive view of consumer trust.

This study, drawing from complexity theory and configurational approach, adds to privacy and e-commerce literature by presenting combinations of causal conditions that affect privacy-related defensive behaviours. Although previous studies have identified different factors leading to defensive behaviour (Lwin et al., 2016; Poddar et al., 2009), this is the first study to apply fsQCA that differentiates from previous regression-based methods that focus on the main effects of different antecedents on a particular outcome but not on interdependencies between those antecedents (Woodside, 2014). The findings revealed that privacy concerns and internet experience are necessary conditions to engage in higher defensive behaviours. These

conditions in combination with other sufficient conditions provide different solutions to explain a high score of defensive behaviours.

Practical implications

There are several managerial implications in this study. Consumer privacy concerns are directly-driven by corporate privacy practices. However, the study identified that privacy concerns are more heavily driven by the way corporations establish a trusting online environment, and to what extent consumers are empowered. Therefore, ensuring trust and empowering consumers are two fundamental strategies that will enable firms to manage privacy concerns as well as minimising the resulting backlash through their responsible privacy practices. The study specially highlights the need for corporations to focus on empowering consumers by re-evaluating their privacy practices. For instance, studies continuously show the shortcomings, such as complexity and lengthiness, of privacy notices (Leon et al., 2012). These shortcomings inhibit consumers from developing a fundamental awareness about how their information is collected and used. Similarly, the use of big data and data analytics has blurred data collecting structures. Thereby, lack of transparency has become a threat to making informed choices and to controlling the information flow (Arli et al., 2018; Petrescu and Krishen, 2018; Yun et al., 2018). Thus, such corporate practices violate the most critical aspects of consumer privacy empowerment that lead to consumers taking defensive actions such as withdrawing from transactions or fabricating their real information. These practices were found to have a similar effect on trust where consumers end up again responding defensively due to their perceptions of online sellers' lack of benevolence, integrity, competence and predictability.

This study identified several antecedents of high consumer defensive behaviours. While we identified some factors as being necessary than others, we also identified configurations

that can help online retailers and policy makers to understand patterns of factors leading consumers to respond defensively. Marketers and policy makers can develop strategies to overcome consumer backlash more effectively by using different configurations identified in this study.

The study findings verify that regulations play a paramount role in maintaining 'market equalisation' in terms of information exchange for privacy protection and fair use of consumer information for commercial purposes. Both the public pressure and regulatory mechanisms prefer corporations' 'self-policing' their privacy practices (Holtrop et al., 2017). Especially, stringent regulations are required to maintain a trusting information exchange environment, and to empower consumers to manage their privacy. However, the adequacy, ability, and availability of regulations proportionate to the advances in the market are questionable (Petrescu and Krishen, 2018). Some scholars argue that consumers' overall privacy would decline over time, as maintaining their privacy would be costly to consumers (Kannan, 2017). Hence, substantial regulations that can deal with escalating technological changes, consumer vulnerabilities, market inequalities, and marketing malpractices (Kucuk, 2009; Kucuk, 2016) are required. As mentioned earlier, ensuring trust in the marketplace and empowering individual consumers, are two strategies that can help regulators to reduce privacy concerns and consumer backlash.

Future research

This study focused on corporations and regulators as power holders that influence consumer privacy attitudes and behaviours. However, scholars identify that privacy threats are increasingly emerging from the external environment that is beyond the control of corporations, consumers, and regulators (Ferrell, 2017). Future research should take into account the

changing power dynamics caused by unauthorised and illegal entities such as hackers and data brokers.

Privacy concerns are the most widely used factor or construct to predict privacy-related consumer behaviour. This study also highlights the importance of privacy empowerment, which is only nascent in the marketing scholarship. Future studies need to probe into factors that can augment or diminish privacy empowerment. Also, the relationship of empowerment with different behavioural outcomes needs to be further studied.

There are some limitations to the study. The sample was drawn from Australian consumers only. Therefore, the homogeneity of our sample can cause limitations in generalising findings. The cross-country or –culture differences can impact consumer privacy attitudes and behaviours (Chen et al., 2013). Hence, such aspects should be considered in future investigations. Also, this study used cross-sectional data that provides a 'snapshot' of the phenomena under investigation at a specific time frame. With changing technological environment and regulatory policies and mechanisms, for instance, recent enactment of General Data Protection Regulation (GDPR), privacy issues can evolve over time. Longitudinal studies would benefit researchers to understand how power and responsibility dynamics evolve over a certain period of time.

Conclusion

This study offers evidence as to why consumers engage in privacy-related defensive behaviours using the power-responsibility equilibrium theory. Thereby, we provide several insights on how to manage privacy issues to establish a functional and healthy online market for both firms and consumers. We used both PLS-SEM and fsQCA methods to derive direct causal factors as well as configurations of causal conditions to comprehensively explain consumer privacy behaviour. The key finding of the study reveals that lack of corporate privacy responsibility

and regulatory protection can deprive consumers of privacy empowerment, and damage consumer trust, thus triggering privacy concerns and subsequent defensive responses. We provide several theoretical and practical implications to extend the privacy scholarship as well as to improve privacy protection in the digital marketplace.

References

Akhter, S. H. (2014), "Privacy concern and online transactions: The impact of internet self-efficacy and internet involvement", *Journal of Consumer Marketing*, Vol. 31 No. 2, pp. 118-125.

Akter, S., D'Ambra, J. and Ray, P., (2011), "Trustworthiness in mHealth information services: an assessment of a hierarchical model with mediating and moderating effects using partial least squares (PLS) ", *Journal of the American Society for Information Science and Technology*, Vol. 62 No. 1, pp.100-116.

Akter, S., Fosso Wamba, S. and Dewan, S. (2017), "Why PLS-SEM is suitable for complex modelling? An empirical illustration in big data analytics quality", *Production Planning and Control*, Vol. 28 No. 11-12, pp. 1011-1021.

Arli, D., Bauer, C. and Palmatier, R. W. (2018), "Relational selling: Past, present and future", *Industrial Marketing Management*, Vol. 69, pp. 169-184.

Awad, N. F. and Krishnan, M. S. (2006), "The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization", *MIS Quarterly*, Vol. 30 No. 1, pp. 13-28.

Bandara, R., Fernando, M. and Akter, S. (2019), "Privacy concerns in e-commerce: A taxonomy and a future research agenda", *Electronic Markets*. doi: https://doi.org/10.1007/s12525-019-00375-6

Bandara, R., Fernando, M. and Akter, S. (2020a), "Addressing privacy predicaments in the digital marketplace: A power-relations perspective", *International Journal of Consumer Studies*. doi: https://doi.org/10.1111/ijcs.12576

Bandara, R., Fernando, M. and Akter, S. (2020b), "Explicating the privacy paradox: A qualitative inquiry of online shopping consumers", *Journal of Retailing and Consumer Services,* Vol. 52, pp. 1-9.

Caudill, E. M. and Murphy, P. E. (2000), "Consumer online privacy: Legal and ethical issues", *Journal of Public Policy & Marketing,* Vol. 19 No. 1, pp. 7-19.

Chen, J. Q., Zhang, R. and Lee, J. (2013), "A cross-culture empirical study of m-commerce privacy concerns", *Journal of Internet Commerce,* Vol. 12 No. 4, pp. 348-364.

Cheshire, C., Antin, J. and Churchill, E. (2010), "Behaviors, adverse events, and dispositions: An empirical study of online discretion and information control", *Journal of the American Society for Information Science and Technology,* Vol. 61 No. 7, pp. 1487-1501.

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

Culnan, M. J. and Armstrong, P. K. (1999), "Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation", *Organization Science,* Vol. 10 No. 1, pp. 104-115.

Culnan, M. J. and Bies, R. J. (2003), "Consumer privacy: Balancing economic and justice considerations", *Journal of Social Issues,* Vol. 59 No. 2, pp. 323-342.

Davis, K., Frederick, W. C. and Blomstrom, R. L. (1980), *Business and society: Concepts and policy issues,* McGraw-Hill, New York, NY.

Dinev, T. and Hart, P. (2004), "Internet privacy concerns and their antecedents - measurement validity and a regression model", *Behaviour & Information Technology,* Vol. 23 No. 6, pp. 413-422.

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

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.

Ferrell, O. C. (2017), "Broadening marketing's contribution to data privacy", *Journal of the Academy of Marketing Science,* Vol. 45 No. 2, pp. 160-163.

Fiss, P. C. (2011), "Building better causal theories: A fuzzy set approach to typologies in organization research", *Academy of Management Journal,* Vol. 54 No. 2, pp. 393-420.

Flyverbom, M., Deibert, R. and Matten, D. (2019), "The Governance of Digital Technology, Big Data, and the Internet: New Roles and Responsibilities for Business", *Business & Society,* Vol. 58 No. 1, pp. 3-19.

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

Hair Jr, J. F., Hult, G. T. M., Ringle, C. and Sarstedt, M. (2017), *A primer on partial least squares structural equation modeling (PLS-SEM),* Sage Publications, London, UK.

Hair Jr, J. F., Risher, J. J., Sarstedt, M. and Ringle, C. M. (2019a), "When to use and how to report the results of PLS-SEM", *European Business Review,* Vol. 31 No. 1, pp. 2-24.

Hair Jr, J. F., Sarstedt, M. and Ringle, C. M. (2019b), "Rethinking some of the rethinking of partial least squares", *European Journal of Marketing,* Vol. 53 No. 4, pp. 566-584.

Hayes, A. F. (2017), *Introduction to mediation, moderation, and conditional process analysis: A regression-based approach,* Guilford Publications, New York, NY.

Holtrop, N., Wieringa, J. E., Gijsenberg, M. J. and Verhoef, P. C. (2017), "No future without the past? Predicting churn in the face of customer privacy", *International Journal of Research in Marketing,* Vol. 34 No. 1, pp. 154-172.

Hunter, G. L. and Garnefeld, I. (2008), "When does consumer empowerment lead to satisfied customers? Some mediating and moderating effects of the empowerment-satisfaction link", *Journal of Research for Consumers,* No. 15, pp. 1-14.

Kannan, P. K. (2017), "Digital marketing: A framework, review and research agenda", *International Journal of Research in Marketing,* Vol. 34 No. 1, pp. 22-45.

Kim, D. J., Ferrin, D. L. and Rao, H. R. (2008a), "A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents", *Decision Support Systems,* Vol. 44 No. 2, pp. 544-564.

Kim, D. J., Steinfield, C. and Lai, Y.-J. (2008b), "Revisiting the role of web assurance seals in business-to-consumer electronic commerce", *Decision Support Systems,* Vol. 44 No. 4, pp. 1000-1015.

Kim, K. and Kim, J. (2011), "Third-party privacy certification as an online advertising strategy: An investigation of the factors affecting the relationship between third-party certification and initial trust", *Journal of Interactive Marketing,* Vol. 25 No. 3, pp. 145-158.

King, N. J. and Forder, J. (2016), "Data analytics and consumer profiling: Finding appropriate privacy principles for discovered data", *Computer Law & Security Review,* Vol. 32 No. 5, pp. 696-714.

Kock, N. (2015), "Common method bias in PLS-SEM: A full collinearity assessment approach", *International Journal of e-Collaboration,* Vol. 11 No. 4, pp. 1-10.

Krishen, A. S., Raschke, R. L., Close, A. G. and Kachroo, P. (2017), "A power-responsibility equilibrium framework for fairness: Understanding consumers' implicit privacy concerns for location-based services", *Journal of Business Research*, Vol. 73, pp. 20-29.

Kshetri, N. (2014), "Big data′ s impact on privacy, security and consumer welfare", *Telecommunications Policy*, Vol. 38 No. 11, pp. 1134-1145.

Kucuk, S. U. (2009), "The evolution of market equalization on the Internet", *Journal of Research for Consumers*, No. 16, pp. 1-15.

Kucuk, S. U. (2016), "Consumerism in the digital age", *Journal of Consumer Affairs*, Vol. 50 No. 3, pp. 515-538.

Laczniak, G. R. and Murphy, P. E. (1993), *Ethical marketing decisions: The higher road*, Prentice Hall, Upper Saddle River, NJ.

Lai, Y., Sun, H. and Ren, J. (2018), "Understanding the determinants of big data analytics (BDA) adoption in logistics and supply chain management: An empirical investigation", *The International Journal of Logistics Management*, Vol. 29 No. 2, pp. 676-703.

Lee, H., Park, H. and Kim, J. (2013), "Why do people share their context information on Social Network Services? A qualitative study and an experimental study on users' behavior of balancing perceived benefit and risk", *International Journal of Human-Computer Studies*, Vol. 71 No. 9, pp. 862-877.

Leon, P. G., Cranshaw, J., Cranor, L. F., Graves, J., Hastak, M., Ur, B. and Xu, G. (2012), "What do online behavioral advertising privacy disclosures communicate to users?", in *Proceedings of the 2012 ACM workshop on Privacy in the electronic society*, New York, NY, pp. 19-30.

Liao, C., Liu, C.-C. and Chen, K. (2011), "Examining the impact of privacy, trust and risk perceptions beyond monetary transactions: An integrated model", *Electronic Commerce Research and Applications*, Vol. 10 No. 6, pp. 702-715.

Lwin, M., Wirtz, J. and Stanaland, A. J. S. (2016), "The privacy dyad", *Internet Research*, Vol. 26 No. 4, pp. 919-941.

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.

MacKenzie, S. B., Podsakoff, P. M. and Podsakoff, N. P. (2011), "Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques", *MIS Quarterly*, Vol. 35 No. 2, pp. 293-334.

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

Martin, K. (2016a), "Data aggregators, consumer data, and responsibility online: Who is tracking consumers online and should they stop?", *The Information Society*, Vol. 32 No. 1, pp. 51-63.

Martin, K. (2016b), "Understanding privacy online: Development of a social contract approach to privacy", *Journal of Business Ethics*, Vol. 137 No. 3, pp. 551-569.

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.

Martin, K. D. and Murphy, P. E. (2017), "The role of data privacy in marketing", *Journal of the Academy of Marketing Science*, Vol. 45 No. 2, pp. 135-155.

McKnight, D. H. and Chervany, N. L. (2001), "What trust means in e-commerce customer relationships: An interdisciplinary conceptual typology", *International Journal of Electronic Commerce,* Vol. 6 No. 2, pp. 35-59.

McKnight, D. H., Choudhury, V. and Kacmar, C. (2002), "The impact of initial consumer trust on intentions to transact with a web site: A trust building model", *The Journal of Strategic Information Systems,* Vol. 11 No. 3, pp. 297-323.

Midha, V. (2012), "Impact of consumer empowerment on online trust: An examination across genders", *Decision Support Systems,* Vol. 54 No. 1, pp. 198-205.

Miltgen, C. L., Henseler, J., Gelhard, C. and Popovič, A. (2016), "Introducing new products that affect consumer privacy: A mediation model", *Journal of Business Research,* Vol. 69 No. 10, pp. 4659-4666.

Miltgen, C. L. and Smith, H. J. (2015), "Exploring information privacy regulation, risks, trust, and behavior", *Information & Management,* Vol. 52 No. 6, pp. 741-759.

Morey, T., Forbath, T. and Schoop, A. (2015), "Customer data: Designing for transparency and trust", *Harvard Business Review,* Vol. 93 No. 5, pp. 96-105.

Morrison, E. W. and Robinson, S. L. (1997), "When employees feel betrayed: A model of how psychological contract violation develops", *Academy of Management Review,* Vol. 22 No. 1, pp. 226-256.

Mou, J., Shin, D.-H. and Cohen, J. F. (2017), "Trust and risk in consumer acceptance of e-services", *Electronic Commerce Research,* Vol. 17 No. 2, pp. 255-288.

Mousavizadeh, M., Kim, D. J. and Chen, R. (2016), "Effects of assurance mechanisms and consumer concerns on online purchase decisions: An empirical study", *Decision Support Systems,* Vol. 92, pp. 79-90.

Murphy, P. E., Laczniak, G. R., Bowie, N. E. and Klein, T. A. (2005), *Ethical marketing,* Prentice-Hall, Upper Saddle River, NJ.

Pappas, I. O. (2018), "User experience in personalized online shopping: a fuzzy-set analysis", *European Journal of Marketing,* Vol. 52 No. 7/8, pp. 1679-1703.

Pappas, I. O., Kourouthanassis, P. E., Giannakos, M. N. and Chrissikopoulos, V. (2016), "Explaining online shopping behavior with fsQCA: The role of cognitive and affective perceptions", *Journal of Business Research,* Vol. 69 No. 2, pp. 794-803.

Peer, E., Vosgerau, J. and Acquisti, A. (2014), "Reputation as a sufficient condition for data quality on Amazon Mechanical Turk", *Behavior Research Methods,* Vol. 46 No. 4, pp. 1023-1031.

Perkins, D. D. and Zimmerman, M. A. (1995), "Empowerment theory, research, and application", *American Journal of Community Psychology,* Vol. 23 No. 5, pp. 569-579.

Petrescu, M. and Krishen, A. S. (2018), "Analyzing the analytics: data privacy concerns", *Journal of Marketing Analytics,* Vol. 6 No. 2, pp. 41-43.

Poddar, A., Mosteller, J. and Ellen, P. S. (2009), "Consumers' rules of engagement in online information exchanges", *Journal of Consumer Affairs,* Vol. 43 No. 3, pp. 419-448.

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

Pollach, I. (2011), "Online privacy as a corporate social responsibility: An empirical study", *Business Ethics: A European Review,* Vol. 20 No. 1, pp. 88-102.

Preacher, K. J. and Hayes, A. F. (2008), "Asymptotic and resampling strategies for assessing and comparing indirect effects in multiple mediator models", *Behavior Research Methods,* Vol. 40 No. 3, pp. 879-891.

Queiroz, M. M. and Wamba, S. F. (2019), "Blockchain adoption challenges in supply chain: An empirical investigation of the main drivers in India and the USA", *International Journal of Information Management,* Vol. 46, pp. 70-82.

Ragin, C. C. (2008), *Redesigning social inquiry: Fuzzy sets and beyond,* University of Chicago Press, Chicago.

Ragin, C. C. (2018), *User's Guide to Fuzzy-Set/Qualitative Comparative Analysis 3.0,* Department of Sociology, University of California, Irvine, California.

Rousseau, D. M., Sitkin, S. B., Burt, R. S. and Camerer, C. (1998), "Not so different after all: A cross-discipline view of trust", *Academy of Management Review,* Vol. 23 No. 3, pp. 393-404.

Schaerer, M., du Plessis, C., Yap, A. J. and Thau, S. (2018), "Low power individuals in social power research: A quantitative review, theoretical framework, and empirical test", *Organizational Behavior and Human Decision Processes,* Vol. 149, pp. 73-96.

Shmueli, G., Sarstedt, M., Hair, J. F., Cheah, J.-H., Ting, H., Vaithilingam, S. and Ringle, C. M. (2019), "Predictive model assessment in PLS-SEM: guidelines for using PLSpredict", *European Journal of Marketing,* Vol. 53 No. 11, pp. 2322-2347.

Son, J.-Y. and Kim, S. S. (2008), "Internet users' information privacy-protective responses: A taxonomy and a nomological model", *MIS Quarterly,* Vol. 32 No. 3, pp. 503-529.

Spreitzer, G. M. (1995), "Psychological empowerment in the workplace: Dimensions, measurement, and validation", *Academy of Management Journal,* Vol. 38 No. 5, pp. 1442-1465.

Stanaland, A. J., Lwin, M. O. and Murphy, P. E. (2011), "Consumer perceptions of the antecedents and consequences of corporate social responsibility", *Journal of Business Ethics,* Vol. 102 No. 1, pp. 47-55.

Stewart, D. W. (2017), "A comment on privacy", *Journal of the Academy of Marketing Science,* Vol. 45 No. 2, pp. 156-159.

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

Thomas, K. W. and Velthouse, B. A. (1990), "Cognitive elements of empowerment: An "interpretive" model of intrinsic task motivation", *Academy of Management Review,* Vol. 15 No. 4, pp. 666-681.

Tsou, H.-T. and Hsu, S. H.-Y. (2015), "Performance effects of technology–organization–environment openness, service co-production, and digital-resource readiness: The case of the IT industry", *International Journal of Information Management,* Vol. 35 No. 1, pp. 1-14.

van Dyke, T., Midha, V. and Nemati, H. (2007), "The effect of consumer privacy empowerment on trust and privacy concerns in e-commerce", *Electronic Markets,* Vol. 17 No. 1, pp. 68-81.

Wang, T., Duong, T. D. and Chen, C. C. (2016), "Intention to disclose personal information via mobile applications: A privacy calculus perspective", *International Journal of Information Management,* Vol. 36 No. 4, pp. 531-542.

West, S. M. (2019), "Data capitalism: Redefining the logics of surveillance and privacy", *Business & Society,* Vol. 58 No. 1, pp. 20-41.

Wirtz, J. and Lwin, M. O. (2009), "Regulatory focus theory, trust, and privacy concern", *Journal of Service Research,* Vol. 12 No. 2, pp. 190-207.

Wirtz, J., Lwin, M. O. and Williams, J. D. (2007), "Causes and consequences of consumer online privacy concern", *International Journal of Service Industry Management,* Vol. 18 No. 4, pp. 326-348.

Woodside, A. G. (2013), "Moving beyond multiple regression analysis to algorithms: Calling for adoption of a paradigm shift from symmetric to asymmetric thinking in data analysis and crafting theory", *Journal of Business Research,* Vol. 4 No. 66, pp. 463-472.

Woodside, A. G. (2014), "Embrace• perform• model: Complexity theory, contrarian case analysis, and multiple realities", *Journal of Business Research,* Vol. 67 No. 12, pp. 2495-2503.

Wu, K.-W., Huang, S. Y., Yen, D. C. and Popova, I. (2012), "The effect of online privacy policy on consumer privacy concern and trust", *Computers in Human Behavior,* Vol. 28 No. 3, pp. 889-897.

Xu, H., Dinev, T., Smith, J. and Hart, P. (2011), "Information privacy concerns: Linking individual perceptions with institutional privacy assurances", *Journal of the Association for Information Systems,* Vol. 12 No. 12, pp. 798-824.

Youn, S. (2009), "Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents", *Journal of Consumer affairs,* Vol. 43 No. 3, pp. 389-418.

Yun, H., Lee, G. and Kim, D. J. (2018), "A chronological review of empirical research on personal information privacy concerns: An analysis of contexts and research constructs", *Information & Management,* Vol. Online.

Zimmerman, M. A. (1995), "Psychological empowerment: Issues and illustrations", *American Journal of Community Psychology,* Vol. 23 No. 5, pp. 581-599.

Zwitter, A. (2014), "Big data ethics", *Big Data & Society,* Vol. 1 No. 2, pp. 1-6.

Appendices

Appendix A: Constructs and measurement items

Construct and measurement sources	Measurement Items
Privacy Concerns (Miltgen et al., 2016; Mousavizadeh et al., 2016)	I am concerned that: My online behaviour and activities can be monitored/tracked without my permission Online sellers are collecting personally identifiable information without my permission Online sellers could use my personal information for other purposes without my authorisation Online sellers share my personal information with different parties without my agreement Online sellers could store my personal information for years without my permission Online sellers could create a detailed profile about me using personal data from various sources without my knowledge

Trust (Dinev et al., 2006; Malhotra et al., 2004)	I trust online sellers keep my best interests in mind when dealing with my information
	Online sellers handle my personal information in a competent manner
	Online sellers are honest in using my information
	Online sellers are predictable regarding the usage of my information
	The Internet is a safe and reliable place to exchange information with online sellers
Privacy Empowerment (Cheshire et al., 2010; Kim and Kim, 2011; Spreitzer, 1995; Youn, 2009)	I have control over what happens to my personal information once it is given to online sellers
	I have choices as to how my personal information is used by online sellers beyond transactions
	I am highly aware of technologies or practices used by online sellers which may invade my privacy
	I feel confident protecting my online privacy
	I have significant influence over how my personal information is used by online sellers
	Overall, I feel helpless about how online sellers collect and use my personal information (reverse coded)

Corporate Privacy Responsibility (Son and Kim, 2008; Stanaland et al., 2011)	Online sellers provide clear and understandable terms and conditions about how my information is used
	Online sellers always take my consent before collecting and using my personal information for different purposes
	Online sellers' use of my information is transparent
	Online sellers' use of my information is ethical
	Online sellers' use of my information is fair
	Online sellers act responsibly in protecting my privacy
Regulatory Protection (Dinev et al., 2013; Lwin et al., 2007; Xu et al., 2011)	Existing laws in Australia are sufficient to protect my online privacy
	The government is doing enough to ensure consumers are protected against online privacy violations
	The law is capable of governing practices of how online sellers collect, use, and protect my information
	There are strong international laws to protect personal information of individuals on the Internet
	Third party seals and certificates (e.g. TrustMark) are able to ensure my online privacy

Defensive Behaviour (Lwin et al., 2007; Lwin et al., 2016; Youn, 2009)	How often do you take the following protective actions?
	Falsify some of your personal information when asked by online companies
	Provide incomplete information
	Use measures to avoid sellers' tracking your browsing behaviour
	Use software or applications to protect online privacy
	Refuse to give information to online companies when you think it is too personal
	Use online sellers who do not ask for too much information

Appendix B: Correlation matrix (Fornell-Larcker criteria)

	(1)	(2)	(3)	(4)	(5)	(6)
(1) Privacy Concerns	**0.796**					
(2) Trust	-0.699	**0.814**				
(3) Privacy Empowerment	-0.699	0.678	**0.758**			
(4) Corporate Privacy Responsibility	-0.673	0.692	0.651	**0.766**		
(5) Regulatory Protection	-0.650	0.686	0.624	0.685	**0.797**	
(6) Defensive Behaviour	0.674	-0.650	-0.651	-0.547	-0.554	**0.769**

*Diagonal values (in bold) are the square root AVE.

Appendix C: Heterotrait-Monotrait Ratio (HTMT) statistic

	(1)	(2)	(3)	(4)	(5)	(6)
(1) Privacy Concerns						
(2) Trust	0.791					
(3) Privacy Empowerment	0.805	0.783				
(4) Corporate Privacy Responsibility	0.772	0.796	0.759			
(5) Regulatory Protection	0.744	0.781	0.725	0.793		
(6) Defensive Behaviour	0.769	0.745	0.756	0.630	0.636	