Journal of Retailing and Consumer Services 52 (2020) 101947

Contents lists available at ScienceDirect

Journal of Retailing and Consumer Services

journal homepage: www.elsevier.com/locate/jretconser

Explicating the privacy paradox: A qualitative inquiry of online shopping consumers

Ruwan Bandara[a,*], Mario Fernando[a], Shahriar Akter[b]

[a] School of Management, Operations, & Marketing, Faculty of Business, University of Wollongong, Northfields Ave, Wollongong, NSW, 2522, Australia
[b] Sydney Business School, University of Wollongong, NSW, Australia

ARTICLE INFO

Keywords:
Consumer online privacy
Privacy paradox
Online shopping

ABSTRACT

Online consumers often voice discontent and concern over their privacy and yet fail to take adequate precautions. Nor do they abstain from disclosing information. This study aims to explore this phenomenon which is known as the privacy paradox. Based on semi-structured interviews with online shopping consumers and thematic analysis of data, this paper illuminates the privacy paradox using three themes: psychological distance of privacy, perceived social contracts of privacy, and learned helplessness and privacy empowerment. Our findings contribute to the privacy paradox discourse and provide several implications for consumers, online retailers, and policymakers.

1. Introduction

The ubiquitous, widespread use of the internet and advent of new technologies continue to be a game-changer for retailing. Especially, e-commerce has emerged as a strong alternate of physical commerce with global e-commerce retail reaching nearly 1.66 billion people in 2017 (Statista, 2018b). In the US alone, e-commerce retail sales reached $336 billion in 2017 (Statista, 2018a).

Although the internet has enabled retailers to reach new markets and new consumers, retaining them and earning their long-term trust and loyalty have become a challenge (Fransi and Viadiu, 2007). Especially, safeguarding consumer privacy is a crucial impediment for the growth of e-commerce. Privacy is germane to the flow of information—what, by whom, why, and how information is collected and used (Martin, 2016b). Owing to the seismic shift in the collection, storage, mining, and commoditization of consumer data, concerns over online privacy have multiplied (Arli et al., 2018; Martin and Murphy, 2017; Petrescu and Krishen, 2018). Use of rich and robust consumer digital profiles has enabled companies to predict consumer behavior and provide highly personalized and customized services and thereby generate new business value (Holtrop et al., 2017; Petrescu and Krishen, 2018). However, there is a fine line between data-driven marketing efforts (e.g., targeted advertising, data mining) and protection of consumer privacy (Arli et al., 2018; Holtrop et al., 2017; Schneider et al., 2017). So in order to establish a consumer-friendly digital marketplace, it is essential that we understand privacy dynamics including consumer privacy perceptions and their behaviors.

Understanding consumer privacy becomes a further necessity, given the perplexing nature of their privacy-related behaviors. Prior research indicates that despite online consumers' concerns and worries over privacy, they at times readily divulge their personal information, accept being tracked and profiled, and fail to take adequate protective measures (Baruh et al., 2017; Berendt et al., 2005; Kokolakis, 2017; Norberg et al., 2007). This anomaly, by which consumers behave contrary to their privacy attitudes or stated privacy concerns, is widely known as the privacy paradox (Dienlin and Trepte, 2015; Norberg et al., 2007).

In the online retailing context, consumers face an essential trade-off— consumers are required to provide at least a minimum amount of information to perform a transaction and face the risks associated with disclosing their information (Boritz and No, 2011). Also, the need for online consumers to divulge an honest account of their personal information to obtain products and services is unavoidable. Beyond these reasons, the privacy paradox phenomenon highlights the necessity of research to scrutinize consumer privacy issues including the legitimacy of privacy concerns, the ways individuals perceive privacy and explore consumer awareness about the extensiveness of privacy invasive mechanisms and practices (Dinev, 2014; Norberg et al., 2007).

The privacy paradox renders several implications for consumers, marketers, and online retailers but only a few studies have focused on illuminating the privacy paradox in the marketing discipline. The privacy paradox can have menacing repercussions on individual consumers; the notion of a privacy paradox can result in cruder collection

* Corresponding author.
E-mail addresses: hmrjb180@uowmail.edu.au (R. Bandara), mariof@uow.edu.au (M. Fernando), sakter@uow.edu.au (S. Akter).

https://doi.org/10.1016/j.jretconser.2019.101947
Received 9 May 2019; Received in revised form 28 August 2019; Accepted 9 September 2019
Available online 03 October 2019

and use of consumer data and less restrictive privacy regulations threatening individual privacy (Martin and Nissenbaum, 2016). On the other hand, the misperception of consumer privacy issues may waste online retailers' marketing efforts, tarnish consumer-vendor relationships, and impede retailers' strategy of using protection of privacy as a competitive advantage.

The objective of this study is to explore the determinants of privacy paradox in the online shopping context. This paper specifically addresses the following research question: Why do consumers undermine their privacy interests when shopping online? We use a qualitative research design based on semi-structured interviews to answer this question. This paper extends the understanding of the privacy paradox beyond economic explanations—a trade-off which consumers surrender their privacy for perceived benefits. Thereby, this paper contributes to the literature by illuminating the privacy paradox as a result of (1) psychological distance of privacy, (2) learned helplessness and lack of consumer privacy empowerment, and (3) perceived social contracts of privacy.

In the following sections, we provide a review of relevant literature, elaborate on the methods used in our study, and provide a detailed illustration of the themes found in the analysis. The paper concludes with a discussion including implications for research and practice, and study limitations.

2. Literature review

2.1. Privacy paradox

It has taken the attention of scholars from several disciplines to probe what causes consumers to undermine their privacy when behaving online (Barth and de Jong, 2017; Gerber et al., 2018; Kokolakis, 2017). Studies in different contexts including online shopping and online social networking provide numerous insights. Most explanations are based on economic and social determinants, while few studies have focused on other aspects such as psychological determinants (Kokolakis, 2017). Individual decision-making as determined by risk-benefit calculation is well established in the privacy scholarship. Privacy paradox studies are also largely influenced by this approach, rooted in theories such as privacy calculus theory (Culnan and Armstrong, 1999) and rational choice theory of human behavior (Simon, 1955). The central thesis of this approach is that decisions are made rationally with conscious and analytical thinking. Accordingly, consumers rationally make a calculus or trade-off between potential gains and losses of sharing their information. Several studies have found that economic and social benefits of information disclosure undermine the consumer concerns over privacy (e.g., Berendt et al., 2005; Lee and Kwon, 2015). For instance, a consumer may divulge sensitive information despite his or her concerns over privacy to receive personalized online services. Therefore, the dichotomy between privacy concerns and behavior is explained as an over-emphasis or prominence of benefits in the calculus process.

Privacy paradox researchers have also probed into the social aspects of privacy decision making. Zafeiropoulou et al. (2013) identify privacy decisions as part of a process of social structuration: a consumer's choice might be to not disclose information, but social structures require such disclosure. For instance, even if consumers' have concerns about disclosing their location data, they might be compelled to reveal such information when downloading a mobile app to access retailer functions. Social influence on privacy decisions can be further demonstrated by peer group pressure where individuals are obliged to share information to achieve conformity and to avoid exclusion (e.g., Taddei and Contena, 2013). However, despite peer or structural pressure, individual motivational factors such as identity construction, social representation, social capital, and relationship management can outweigh concerns over threats to privacy (Debatin et al., 2009; Ellison et al., 2011).

Another domain of privacy paradox studies driven-by behavioral economic theories, highlights the influence of mental biases, heuristics, affect, and limited cognitive resources on privacy decision making (e.g., Hallam and Zanella, 2017; Li et al., 2017). The central thesis of this approach is that decisions are not always made consciously and analytically. They can be preconscious, emotional, immediate, and experienced-based (Novak and Hoffman, 2008). Individuals can be rational only within the walls of their cognitive ability (bounded rationality; Simon, 1982). This is determined by knowledge limitations, time constraints and information asymmetries when making decisions. Hence, individuals tend to misinterpret or inaccurately predict privacy violations leading them to misjudge the overall risk-benefit calculation (Acquisti and Grossklags, 2005). These cognitive limitations can provoke decisions to rely on heuristics. For instance, affect heuristic – a mental shortcut that allows individuals to make decisions based on their affective impressions – can drive an online consumer to disclose more information due to their liking for the website where they shop (Li et al., 2017). While such heuristics enable individuals to make decisions quickly, they can also lead to certain biases. For instance, factors such as immediate gratification and hyperbolic discounting can influence an online consumer to inordinately discount future risk of a privacy violation over more immediate benefits when shopping online (Acquisti, 2004). Therefore, this line of research highlights that the privacy paradox cannot be explained simply as the result of a rational cost-benefit calculation.

To position our findings on a valid theoretical foundation, we particularly focus on three theories. They are introduced below.

2.2. Social contract view of privacy

Privacy has been conceptualized in several ways including privacy as an absolute *right*, as *control*, and as limited *access* to one's information (Martin and Murphy, 2017). These universal and static approaches to privacy rely on the assumption that sharing information is equal to relinquishing one's privacy (Martin, 2016a). The social contract approach to privacy (Culnan and Bies, 2003; Martin, 2016b) contradicts the static and universal approaches to privacy and claims that individuals discriminately share information while having reasonable expectation about privacy to make relationships, to socialize or even trade, with norms governing what, by whom, why, and how their information is used. It also differs from the commodity view of privacy that asserts individuals' privacy decisions are based on rationally calculated risks and benefits (Culnan and Armstrong, 1999). The social contract view rather claims that privacy is governed by social contracts and norms in a particular context. These could include procedural or hypothetical norms in the exchange context.

Based on the social contract view of privacy, we establish that consumers who consider privacy as a social contract, despite concerns for their privacy, will continue to disclose their information relying on procedural, hypothetical contracts and moral norms, expecting that their information will be used within minimal contract standards. For instance, despite consumers' concerns over transacting online, those consumers will share their personal information in order to complete the transaction relying on the contracts governing such transactions.

2.3. Construal level theory (CLT) of psychological distance

Construal level indicates how people encode or mentally represent things. CLT provides a rigorous theoretical basis to understand cognitions and behaviors based on the level of construal. CLT asserts that mental representations are based on psychological distance—the subjective distance of an object or event from an individual's direct immediate reality of the here and now (Liberman et al., 2007; Liberman and Trope, 2008; Trope and Liberman, 2010). According to CLT, mental representations can vary from abstract to concrete. When something is perceived as psychologically distant it forms abstract, decontextualized,

coherent, and superordinate mental representations (high-level construal). On the contrary, when something is perceived as psychologically proximal, it brings into mind more concrete, contextual, and incidental features (low-level construal). The level of construal and psychological distance is reciprocal—"more distant objects will be construed at a higher level, and high-level construal will bring to mind more distant objects" (Trope and Liberman, 2010, p. 444).

Several aspects of psychological distance are discussed. Spatial distance is manifested when individuals encounter something that is far away in space (Fujita et al., 2006). Temporal distance indicates things that are farther away in time from the present—things that belong to past or future (Wakslak et al., 2006). Social distance relates to the level of personal closeness to something (Liviatan et al., 2008). Hypothetical distance is determined by the likeliness or probability of things (Wakslak et al., 2006). Therefore, something happened in the past or happening in the future, in a spatially faraway place, related to other people, and that is less likely to happen, results in higher construal that forms abstract mental representations.

The application of CLT in the privacy context is scarce (Bandara et al., 2017; Bandara et al., 2018). Hallam and Zanella (2017) provide evidence on how temporally-near social networking rewards undermine temporally-distant privacy risks. Among some other studies in the online context, Darke et al. (2016) reveal the impact of spatial distance on online distrust and reluctance to purchase while Hartley and Green (2017) identify the influence of temporal and spatial distance on virtual service separability, and Kim et al. (2016) identify the effect of abstract versus concretely framed advertising messages. We assert that compared to the tangible benefits in the online shopping context, consumer perceptions of the intangibility of privacy values, the elusive and temporal distance of privacy harms, the likelihood of experiencing fewer privacy violations at personal level, and lower sensitivity to privacy harms can undermine consumers' privacy concerns when making decisions in the online context.

2.4. Psychological empowerment and learned helplessness

The concept of empowerment has been examined in numerous contexts and its definitions abound. For instance, consumer empowerment refers to a state in which consumers are free to enact citizenship roles in the marketplace where it is possible to pursue their economic and other broader interests (McShane and Sabadoz, 2015). Psychological empowerment involves analysis of empowerment at the individual level (Zimmerman, 1995). Several aspects of empowerment are discussed. It involves processes and outcomes related to control, critical awareness, and participation (Perkins and Zimmerman, 1995) or it can be manifested in four cognitions namely meaning, competence, self-determination, and impact (Spreitzer, 1995). Psychological empowerment theory asserts that psychological empowerment and its facets must be defined based on the context (Spreitzer, 1995; Zimmerman, 1995). Learned helplessness has been identified as the polar opposite of empowerment. Campbell and Martinko (1998, p. 173) define learned helplessness as a "debilitating cognitive state in which individuals often possess the requisite skills and abilities to perform [a certain activity], but exhibit suboptimal performance because they attribute prior failures to causes which they cannot change, even though success is possible in the current environment". Helplessness is a belief in which an individual considers he or she is ineffective and powerless to prevent negative outcomes or to obtain desired outcomes (Maier and Seligman, 1976).

Only few scholars have paid attention to examining privacy empowerment (e.g., van Dyke et al., 2007), though none in the privacy paradox context. Evolving privacy issues have resulted consumers to believe that there are no effective means of managing their personal information and thereby driving them into a state of resignation (Choi et al., 2018). We assert that when consumers perceive that they are ineffective and powerless to prevent threats to their privacy, they will display passivity in protecting their privacy and divulge information despite their worries over privacy.

3. Methods

To examine the motivations and rationale behind individuals' decision to ignore privacy concerns or undermine their privacy values when taking privacy-related decisions, we undertook a qualitative, semi-structured interview method. Qualitative research helps us to understand people's experiences and the meanings they place on a certain phenomenon, event, process, interaction, structure or setting (Silverman, 2011). According to Sofaer (1999, p. 1106), qualitative methods enable us "not only to describe events but to understand how and why the 'same' events are often interpreted in a different, sometimes even conflicting manner, by different stakeholders." These methods have a grip on real-life as they rely on people's own voices and perceptions, and on how they understand and act under different circumstances (Silverman, 2011).

Privacy paradox research is predominantly based on surveys and experiments. Surveys which rely on self-reported behavior are considered ineffective in capturing actual behaviors, and experiments have failed to create a realistic context of individual behavior (Kokolakis, 2017). Hence, both methods have some limitations in generating valid results. According to Kokolakis (2017), limitations in study designs can be a key reason behind misconceptualizing privacy behavior as a paradox. In this study, we used a qualitative method as it allows us to capture rich nuances of responses beyond terms and categories of responses imposed by the researcher and beyond simulated responding conditions – as in survey or experimental research.

3.1. Data collection

With the aim of producing rich data, we conducted semi-structured interviews with online shopping consumers. The respondents were selected using a combination of convenient and snowball sampling techniques (Saunders et al., 2012). Our focus was on understanding the privacy paradox among online shopping consumers in the business to consumer (B2C) e-commerce context. We selected the participants from Australia based on whether they have done online shopping during the last three months and whether participants are above the age of 18 years. Initially, participants were recruited via voluntary basis and also via personal contacts and these participants nominated other potential participants that could engage in the study. We ensured that the sample was diverse in terms of demographics and experience as indicated in Table 1. We conducted a total of 26 interviews that assured the variability of data and thematic saturation (Guest et al., 2006). The interviews were conducted over seven months from April to October 2017. The interviews lasted an average of 40 min.

Table 1
Descriptive statistics of the sample.

	Percentage		Percentage
Age (years)		**Gender**	
18-24 (Group 1)	23	Male	42
25-34 (Group 2)	19	Female	58
35-44 (Group 3)	23	**Education**	
45-54 (Group 4)	12	HSC	8
55 above (Group 5)	23	Degree	35
Online Shopping Experience	Postgraduate Degree	57	
1-4 years	12	**Internet Experience**	
5-8 years	38	6-10 years	15
More than 8 years	50	11-15 years	46
		16-20 years	27
		More than 20 years	12

We ensured the anonymity of the participants' responses in order to elicit honest responses as is necessary for discussion of sensitive topics and to avoid social desirability bias (Merriam and Tisdell, 2016). Written consent was obtained from all the participants, including consent for the interview to be audio recorded.

Our interviews focused on several issues including on privacy attitudes, privacy responses, and privacy paradox. We developed the semi-structured interview guideline (see Appendix) based on prior syntheses of general privacy and privacy paradox literature (e.g., Barth and de Jong, 2017; Dinev et al., 2015; Kokolakis, 2017; Smith et al., 2011). Especially, we were driven by the need to understand why consumers undermine their privacy interests when shopping online. We set the background to the interview by discussing their general perceptions and experiences about online shopping. Then we inquired what they understand by information privacy, knowledge and awareness about privacy issues, the nature of their privacy concerns, and measures taken to protect privacy. We explored the causes behind the privacy paradox by asking them to explain what conditions or causes can make them disregard their values or concerns for privacy. In the following section, we discuss how we analyzed the data to derive the major causes of privacy paradox.

3.2. Data analysis

We considered thematic analysis technique as useful to identify overarching themes pertinent to the privacy paradox. Thematic analysis identifies meanings or threads in a dataset that continually emerge germane to a certain phenomenon or a problem of interest (Braun and Clarke, 2006). These recurrent patterns become the categories for the systematic analysis of that phenomenon (Braun and Clarke, 2006; Fereday and Muir-Cochrane, 2006). We followed a data-driven inductive approach to thematic analysis as it allows themes on the privacy paradox to emerge directly from the data rather than using a specific theory or a priori template of codes (Boyatzis, 1998). In this study, we used QSR NVivo 11 software to ensure accurate coding, management, and analysis of data. We developed the initial nodal structure after the preliminary scan of the data. Open coding was used to identify the first-order codes (Strauss and Corbin, 1998). After the data were coded and collated, they were analyzed to identify how different codes can be grouped into initial categories and we sought for relational structures to narrow down and solidify these categories using axial coding (Strauss and Corbin, 1998). We continually reviewed the literature to confirm categories while allowing new categories to emerge from data. In the next step, we conducted selective coding to develop higher-order categories or themes from initial categories (Strauss and Corbin, 1998). The codes and themes were reviewed at two levels. In the first level, we reviewed the collated extracts for each theme to check whether they appear to form a coherent pattern. In the second level, we reviewed individual themes in relation to the complete data set to reach theme saturation until we did not find any new insights. In addition, an external researcher reviewed the data structure to avoid bias and to improve reliability of the findings (Creswell, 2013). To establish internal validity, member checks were conducted with ten participants for accuracy of themes (Lincoln and Guba, 1985).

The data analysis revealed four major themes to illuminate the privacy paradox. However, this paper only focuses on presenting three novel areas as previous studies have provided substantial evidence on how benefits motivate consumers to undermine their privacy (i.e., privacy calculus).

4. Thematic analysis results

4.1. Perceived social contracts of privacy

Several interviewees defined privacy in contractual terms. An interviewee stated, *"privacy means … I only want the general public or anyone to know the things that I am willing to give out … Unless I have given the information, you shouldn't have it … and using the information in the right way, for the way that I have agreed to"* (female, age group 1).

The social contracts can include perceptions about legal procedures as well as hypothetical and moral norms governing a particular exchange (Martin, 2016b). For instance, consumers divulge their information expecting that the other party will collect and use their information according to the procedural norms and conditions. As declared by an interviewee, *"there is a requirement. You have to disclose your information to a dealer … otherwise you don't get the product you want … There is an understanding that whatever information is given, it will be used according to the requirement of the law, according to the privacy act … or any other requirement"* (male, age group 5).

They also expect online companies will conform to moral norms that govern any particular information exchange. In relying on sellers' ethical use of consumer data, trust plays a critical role – *"I like to think that no one's taking advantage of my information. So for me, I'm willing to give out my information – although it's valuable information, I just have to trust that no one is using that in a negative way. That can seem a bit naïve but if you don't allow for some risk, you won't leave the house basically"* (female, age group 3). Hence, consumers accept vulnerability based on positive expectations about norms governing data practices.

The significance of procedural and hypothetical contracts or norms becomes prominent when consumers deal with unknown or unfamiliar sellers. When asked on what grounds consumers share information with unfamiliar sellers while having risks for privacy, an interviewee declared, *"I think sometimes when we are forming a relationship with people, we will give something of ourselves and hope that we will receive something of the other person and that forms a relationship, we share information with each other. So that's my guess"* (female, age group 3).

Consumers exchange their information for certain needs and benefits including shopping gratification and convenience; consumers are privacy pragmatists (Beales and Muris, 2008). Consumers do not think that sharing information or accepting information vulnerabilities as a matter of ceding their privacy. Rather, they have expectations of what, how, and by whom information is used.

4.2. Learned helplessness and privacy empowerment

When consumers' privacy boundaries are continually invaded and control over their personal information is lost, consumers display a state of resignation or passivity in their privacy behavior. *"Over the great scheme of things I see that we are losing privacy every day. I feel we are not going to ever have it back … And as a result, I am very like, oh well that's life!"* (male, age group 2). Similar responses suggest the idea of learned helplessness over one's privacy.

Participants' lack of control over information is a main reason for learned helplessness. An interviewee mentioned, *"control over information … it's gone. Once you submit [information], your life is not your own anymore"* (female, age group 3) and similarly, *"there is so much data mining that's going on now too. I just don't know where my information is anymore. Because of the ways the companies have to work now and everything is online, we're almost forced into this just to be able to live and to do things"* (female, age group 5). Control reflects one's ability to exert influence over decisions, which according to Spreitzer (1995) is a key element of empowerment.

Having critical awareness about the environment or context in which the decisions are made is a precursor to being empowered (Zimmerman, 1995). Lack of critical awareness can hinder consumers taking informed privacy decisions. Some interviewees stated, *"I am not actually that aware of the laws and regulations. I just tend to rely by myself"* (male, age group 3). Consumers are yet to understand the impact of new technologies on privacy: *"I guess that we are still trying to get our heads around things. The technology is moving so fast … society is still trying to catch up and think it through"* (female, age group 3). Overall, interviewees showed lack of cognizance about the changing privacy

dynamics and understanding of the resources needed to deal with rising privacy issues.

Autonomy or having choices in initiating and regulating one's actions reflects a high level of empowerment (Spreitzer, 1995). In the privacy context, consumers are left with few or no choices. As some interviewees mentioned, *"if you want to be online, there are many long agreements and if you do not agree then you cannot use. [It} leaves very little choice and invades privacy rights if you do agree"* (female, age group 5) and *"I wouldn't fully agree that users have no choice, but the choice isn't often an easy one to make"* (male, age group 1). Even though individuals are concerned over privacy, unless they have choices they feel powerless and end up in a state of learned helplessness.

Data suggests that individuals' notion about their ability to protect privacy is instrumental. According to a participant, *"I didn't grow up with any of this so I'm not like my daughter who has basically always had access to the internet. We didn't have that back in 60s and 70s. It feels uncomfortable, definitely, but you have to adjust because everything is online now"* (female, age group 5). Individuals' self-efficacy or belief in their ability to perform certain actions to achieve desired goals reflects their level of empowerment (Perkins and Zimmerman, 1995).

Interviewees' perceptions about limitations in their knowledge, awareness, and ability, and lack of control, choices, and influence over information use, form the theme of privacy empowerment and learned helplessness in explaining why they cannot behave in accordance with their privacy concerns.

4.3. Psychological distance of privacy

We found the concept of privacy, i.e., as a value or a breach of privacy, to be psychologically distant from consumers' minds, especially when the decisions are made. As one interviewee mentioned, *"with privacy and stuff, I've never really had any issues with it. Maybe one day it will come back to bite me, I don't know … privacy issues don't happen at that moment [of shopping]"* (female, age group 2). By disclosing their information consumers enjoy immediate benefits and gratification for the price of a privacy breach that might occur sometime in the future. Even with individuals who faced privacy violations, as time passes, those experiences become a distant concept in their mind. *"[A breach of privacy is] little bit upsetting and shocking at the time but you come to terms with it because this is the sign of the times"* (female, age group 3). Although consumers have concerns over their privacy, temporally distant privacy values are undermined by more immediate benefits when decisions are made.

An interviewee stated, *"[privacy] is not even very tangible because it's online. It feels very distant to your personal physical world"* (female, age group 1). This suggests that the abstract and intangible nature of privacy cause privacy to be distant from their personal experiences. This is further augmented by the disconnection in the virtual online environment. This is evident when some people compare online with physical shopping experiences. *"I think even though you're giving out personal information, it is more anonymous online. Because who's going to care about one tiny little transaction amongst millions compared to a little [physical] shop"* (female, age group 1). This may encourage consumers to divulge more information despite their overall privacy concerns on the internet. Individuals can form more abstract representation of the same phenomenon when the spatial distance is increased (Fujita et al., 2006).

Several interviewees declared probability of a privacy breach at a personal level to be low. *"There are the benefits, immediate benefits, receiving things that you want … they outweigh the risks, risks that may happen or may not happen, you don't know"* (female, age group 2). In a similar vein, *"I think probably the ratio of that protection with the risk is pretty even because the risk that [a privacy violation] would actually [happen] I guess is quite low"* (female, age group 4). It was evident that when consumers perceive the probability of privacy risks as low, these risks are overwhelmed at the decision-making moment by more certain benefits of information disclosure. Recognizing something as unlikely or uncertain results in individuals perceiving it as hypothetically distant from their minds (Wakslak et al., 2006).

Our data indicates that individuals differentiate the value of privacy between themselves and others. As one interviewee mentioned, *"consumers do not want to know that bad things like privacy violations can happen to them. They just bury their heads in the sand and are then surprised when something bad happens"* (female, age group 5). We found that although people are concerned about their privacy, social distance of privacy is high – *"I haven't talked with friends much about it [privacy things]. It's not a topic of conversation. But online shopping is something easily I do online"* (female, age group 5). This highlights the social distance of privacy –individuals consider the overall impact of privacy to be distant from them and their social groups.

5. Discussion

5.1. An extended view of study findings

Our findings indicate that privacy paradox can stem from different reasons beyond economic reasons, i.e., consumers deciding to relinquish their privacy based on perceived benefits. Smith et al. (2011) presented a macromodel of privacy after summarizing two decades of empirical research on privacy, namely the "Antecedents–Privacy Concerns–Outcomes" model (APCO). This review revealed that the vast majority of privacy research is driven by economic theory built on the assumptions about rationality of human behavior. Later, Dinev et al. (2015) argued that privacy research should take into account behavioral economic models, particularly due to the nature of privacy behaviors which are known to be context dependent and paradoxical. Similar ideas are expressed in business research. For instance, Ariely (2009, p. 78) argues that companies have been "operating on the premise that people—customers, employees, managers—make logical decisions. It's time to abandon that assumption." Based on the elaboration likelihood model, Dinev et al. (2015) proposed an enhanced APCO model to showcase how situational and cognitive limitations (e.g., affect, motivations), and extraneous factors (e.g., peripheral cues) influence and modify privacy relationships.

Drawing on Dinev et al. (2015), we incorporate our findings into the APCO model (see Fig. 1). Based on our findings, we argue that the strength of the relationship between privacy concerns and privacy behavior will be modified by psychological distance of privacy (level of construal), state of privacy empowerment (or helplessness), and perceived social contracts of privacy. Our findings provide justification as to why privacy models should extend beyond economic and rational reasoning to explain privacy attitudes and behavior.

CLT provides valuable theoretical justifications to elucidate discrepancy between attitudes, values, and behaviors (Trope and Liberman, 2010). CLT asserts, things that are psychologically distant are construed at higher levels and these abstract and superordinate construals in return influence a person's distant-future attitudes and behaviors (Eyal and Liberman, 2012). We identify that interviewees' perceptions of less immediacy of privacy harms (temporal aspect), fewer personal privacy experiences and less personal relevance of privacy (social aspect), less likeliness of privacy violations (hypothetical aspect), and intangibility of privacy values or harms (spatial aspect) have induced them to perceive privacy as a psychologically distant concept in their minds. Otherwise, the subjective distance of privacy from consumers' direct immediate reality of the here and now can be considerable. On the other hand, online shopping benefits are perceived as immediate, personally-close, likely, and tangible. Based on CLT we argue that, due to psychologically distant perceptions of privacy, they are construed at a higher level and thereby appeal to individuals' distant-future attitudes but are less attractive in actual or proximal decisions and behaviors.

CLT further clarifies that when faced with a value conflict, in more

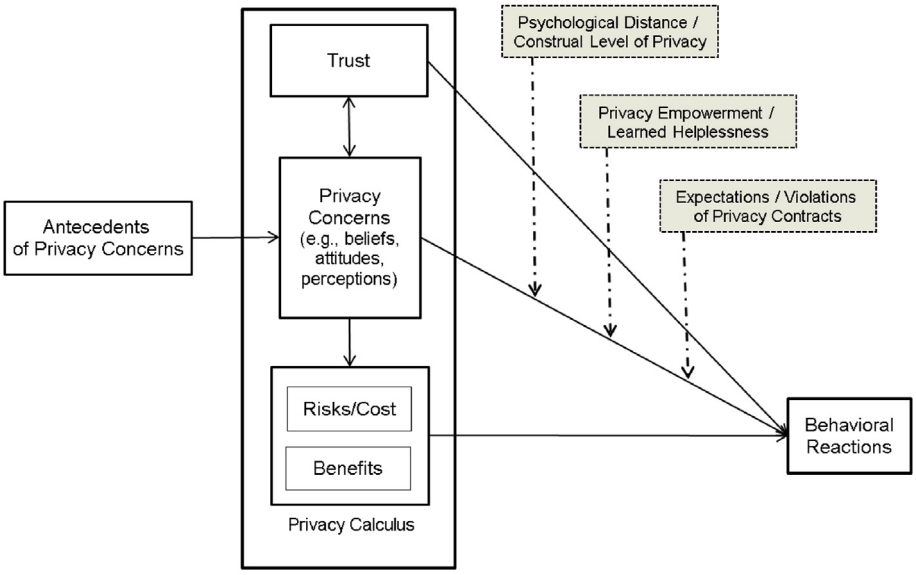

Fig. 1. An extended view of study findings.

immediate situations, a person's secondary values become prominent for their decisions while the central values of a person, which involve higher-level construal, are more influential in distant thinking (i.e., intentions). Accordingly, we argue that privacy as a central value may appeal to individuals when they form attitudes (i.e., privacy concerns) but secondary values such as gratification may overwhelm these when actual shopping decisions are made.

CLT also provides another potential angle to investigate the privacy paradox based on desirability—why we do something—and feasibility—how we do something. Studies on CLT reveal that people tend to consider the desirability of an action over its feasibility as the psychological distance of that particular activity increases and vice versa (Eyal and Liberman, 2012; Liberman et al., 2007). In the privacy context, consumers may have the desire to protect privacy in their distant thinking, but feasibility becomes eminent in the actual use of online services. As we discussed earlier, with the proliferation of privacy-invasive technologies, consumers' ability to protect their privacy and the feasibility of doing so are becoming increasingly strenuous. This provides another justification as to why consumers do not behave according to their privacy concerns.

Our results indicate that when consumers' privacy boundaries are continually invaded and when they are compelled to perceive they have no more control over their personal information, they display a state of resignation about protecting their privacy. This state of learned helplessness that signifies lack of privacy empowerment (Spreitzer, 1995; Zimmerman, 1995) is ensued by consumer beliefs that they cannot produce desired outcomes and prevent undesired outcomes related to the use of their information. Otherwise, they are ineffective and powerless to prevent threats to their privacy. Overall, lack of control and choices over information use and not having adequate knowledge, awareness, and ability to protect their privacy have conditioned consumers to suppress their privacy concerns and display a state of resignation or passivity. Consumers function within structured power relations and they have become ineffective and powerless to resist or to prevent negative outcomes regarding their privacy (Choi et al., 2018). Hence, we assert that consumers' privacy concerns will not necessarily reflect in their behavior due to lack of privacy empowerment.

Several interviewees identified privacy as a social contract (Culnan and Bies, 2003; Martin, 2016b). Hence, assuming disclosing information or granting access to one's information is relinquishing privacy, as in commodity or access view of privacy, can be a fallacy. Our data indicates that consumers do not necessarily equate sharing information as ceding privacy. They discriminately share information among different parties with norms and contract minimums governing the flow of information. The current data-driven marketplace has become complicated in terms of continually changing technologies, entrance of different market actors, and new systems (Martin and Murphy, 2017). In this background, norms and contracts that govern information exchanges are becoming diluted and challenged. Our results indicate, however, that consumers continue to share their information more often based on hypothetical or moral norms—having expectations that their information will be used within minimum ethical standards. As indicated by privacy empowerment findings, consumers function within established power-structures and are less likely to resist or to have choices to form new rules or norms.

5.2. Implications for research

Our findings on privacy empowerment have several theoretical implications. Empowerment is a contextual phenomenon. We contribute to the literature by identifying different facets of empowerment in the privacy context. We identify privacy empowerment to transcend its current understanding 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. 73). Although having control is a critical condition to feeling empowered, it is not adequate—it requires consumers to have fulfilled several other cognitions including critical awareness, autonomy, and self-efficacy. In spite of the fact that previous studies have identified the significance of these aspects individually, we provide an overarching concept and highlight its relevance to explore the privacy paradox. To date, despite a few attempts to understand the impact of privacy empowerment on individuals' privacy concerns (e.g., Kim and Kim, 2011; van Dyke et al., 2007), investigation of its impact on privacy behavior and privacy paradox is absent. Our findings provide a useful starting point for future investigations.

Our findings contribute to the privacy paradox literature by explaining the effect of construal level and psychological distance biases – temporal, spatial, social, and hypothetical. Previously, Hallam and Zanella (2017) employed CLT to investigate temporal distance effect on the privacy paradox in the social networking context. Our contribution is different as we probe the privacy paradox in the online shopping context and extend their work to include different aspects of psychological distance of privacy. Further, based on level of construal and

psychological distance, we explain the privacy paradox as a result of a value-conflict. We reveal how high-construal and psychologically-distant central values such as privacy are undermined over low-construal, immediate, and proximal secondary values such as shopping gratification in decision-making. We also provide another potential angle to explicate the privacy paradox based on the construal effects on feasibility and desirability of choices. Desires for protecting privacy in psychologically distant thinking can be undermined over feasibility factors in psychologically proximal choices. Our findings identify CLT as a useful theory to generate insightful findings in the privacy paradox domain.

Privacy has been mainly viewed as a right, as a commodity, as control, and as limited access to one's information (Martin and Murphy, 2017). According to these views "individuals are incorrectly assumed to give up a large measure of privacy" or "mistakenly framed as dispositive of relinquishing an expectation of privacy", when they share information (Martin, 2016a, p. 60). Therefore, consumers might share their information while having general concerns for privacy, but with expectations that information will be used within the norms of the context of exchange. Our findings are important as privacy paradox literature provides scant evidence on the application of social contract view and explaining the privacy paradox in terms of procedural and hypothetical norms of the context.

5.3. Implications for practice

As we stated at the beginning, conceiving a privacy paradox can end up in further exploitation of consumer data and enactment of relaxed privacy protection mechanisms (Martin and Nissenbaum, 2016). First, consumers need to be aware of the depth and consequences of their privacy behavior. Their voice and reactiveness against threats to privacy is critical. Especially, this is a challenge as privacy is overwhelmed by other values such as gratification in the shopping context. Currently, big data, data analytics, profiling, and targeted advertising have made online shopping experiences highly personalized and proximal to consumers (Pappas, 2018). Consumers must be aware that privacy can be psychologically distant and that it can negatively influence their privacy decisions.

Organizations need to understand that consumers view their privacy as a contract that has certain embedded expectations regarding the flow of information (Martin, 2016b). Misinterpreting consumer trust as privacy-passivity can have an abysmal effect on businesses. For instance, a consumer might not necessarily disable cookies in a website but trust the company to not install third-party cookies to collect his/her data. Our results indicate consumers' lack of control, influence, and choices over how their information is used by businesses are major constraints to protecting their privacy. This has created a state of helplessness where consumers cannot take proactive measures to protect their privacy. Organizations need to empower consumers to take informed and responsible privacy decisions. Research shows individuals experiencing learned helplessness are passive, withdrawn, and dissatisfied (Martinko and Gardner, 1982). Organizations thus need to understand the role of privacy empowerment in consumer relationship management.

Companies need to design comprehensive privacy empowering systems (e.g., online platforms) with adequate control, choice, and influence given to consumers. As we highlighted earlier, giving choices to consumers is not adequate; the systems need to be comprehensive in terms that consumers need to be able to control the choice set. As argued by Tene and Polonetsky (2012, p. 243), companies can follow processes such as featurization that allow "individuals to declare their own policies, preferences and terms of engagement, and do it in ways that can be automated both for them and for the companies they engage". This will not only empower consumers but also reduce the psychological distance of privacy. Further, actions are required to make privacy a more proximal experience in the online shopping context. Taking a consumer-centric approach to privacy will benefit companies in the long run with increased consumer trust and loyalty, enabling companies to establish privacy as a competitive advantage (Martin and Murphy, 2017). For instance, data analytics are widely used to provide highly-personalized services to consumers (Wieringa et al., 2019). However, privacy issues can create a personalization-privacy paradox leading consumers to leave (Aguirre et al., 2016; Pappas, 2018). Therefore, latest research introduces varied consumer-centric privacy-protective data analytics methods that will sustain consumer-vendor relationships (see Wieringa et al., 2019).

Regulators and policy makers play a critical role in narrowing the gap between privacy concerns and privacy behavior. Currently, online privacy is primarily regulated by law and notice and consent. According to Terpstra et al. (2019), "both systems prohibit reflection on privacy issues from the public at large and restrict the privacy debate to the legal and regulatory domains." It is vital that the general public is included in the privacy debate to facilitate making informed decisions based on social dialogue. Privacy education and privacy awareness can also play a significant role (Brough and Martin, 2019). The enactment of stringent privacy laws, such as the General Data Protection Regulation (GDPR) has forced companies to be more transparent as well as to further consumer control over data (Terpstra et al., 2019). We find such efforts are essential to safeguard consumers from developing a state of learned helplessness and to minimize the psychological distance of privacy.

5.4. Limitations of the study

Our study has some limitations. First, our study was based on the Australian context. Researchers need to be aware of this when generalizing our findings to other countries and cultures. Privacy is a contextual-phenomenon – hence, we recommend that researchers should conduct similar work in different cultural contexts and in different countries to verify our results. Second, we focused on only the online shopping context in our study. A similar inquiry in other contexts such as e-health or social networking, researchers might be able to unravel further insights on the privacy paradox. Also, we focused on consumer privacy issues during their overall online shopping experience, which includes both web and mobile platforms. Future research may reveal additional findings by inquiring privacy paradox in different platforms. Third, we selected the sample using a convenient procedure. This sample may not be widely representative. Future research can use alternative research methods reaching a larger sample to verify our findings. For instance, survey method and quantitative analysis can be used to measure the moderating effects of privacy empowerment and psychological distance between consumer privacy concerns and behaviors using a larger sample. In using such methods, researchers however must be careful to use appropriate techniques to capture actual behaviours of the respondents. Although we did try to minimize social desirability bias, face-to-face interviews may carry a certain level of response bias. Despite these limitations, our findings help extend the discourse on privacy paradox to include alternative explanations beyond the commonly used rational and economic reasons.

Declarations of interest

None.

Funding

None.

Appendix

Interview Guide.

Sample questions
What do you understand by privacy?
How concerned are you about privacy?
Compared to your significant others (e.g., family and friends), how concerned are you about privacy?
How likely are privacy violations to occur?
Are privacy issues real or exaggerated? Why?
Have you recently heard about privacy violations or experienced privacy violations yourself?
Do you have the ability to protect your privacy?
What level of control do you have over information?
What level of power do you have to make decisions about how your information should be used by others?
What steps have you taken to protect privacy when shopping online?
Do you think consumers tend to share their information even when they have concerns over privacy? What can be the reasons?
How cautious or conscious are you about privacy when shopping online?
How important is privacy when taking online shopping decisions?
What conditions or causes can make you disregard your values or concerns of privacy?

Appendix A. Supplementary data

Supplementary data to this article can be found online at https://doi.org/10.1016/j.jretconser.2019.101947.

References

Acquisti, A., 2004. Privacy in electronic commerce and the economics of immediate gratification. In: Proceedings of the 5th ACM Conference on Electronic Commerce, New York.

Acquisti, A., Grossklags, J., 2005. Privacy and rationality in individual decision making. IEEE Secur. Priv. 3 (1), 26–33.

Aguirre, E., Roggeveen, A.L., Grewal, D., Wetzels, M., 2016. The personalization-privacy paradox: implications for new media. J. Consum. Mark. 33, 98–110.

Ariely, D., 2009. The end of rational economics. Harv. Bus. Rev. 87, 78–84.

Arli, D., Bauer, C., Palmatier, R.W., 2018. Relational selling: past, present and future. Ind. Mark. Manag. 69, 169–184.

Bandara, R., Fernando, M., Akter, S., 2017. The privacy paradox in the data-driven marketplace: The role of knowledge deficiency and psychological distance. Procedia Computer Science 121, 562–567. https://doi.org/10.1016/j.procs.2017.11.074.

Barth, S., de Jong, M.D.T., 2017. The privacy paradox–Investigating discrepancies between expressed privacy concerns and actual online behavior–A systematic literature review. Telematics Inf. 34, 1038–1058.

Baruh, L., Secinti, E., Cemalcilar, Z., 2017. Online privacy concerns and privacy management: a meta-analytical review. J. Commun. 67 (1), 26–53.

Bandara, R., Fernando, M., Akter, S., 2018. Is the privacy paradox a matter of psychological distance? An exploratory study of the privacy paradox from a construal level theory perspective. In: Proceedings of the 51st Hawaii International Conference on System Sciences, Hawaii, USA, pp. 3678–3687.

Beales, J.H., Muris, T.J., 2008. Choice or consequences: protecting privacy in commercial information. Univ. Chic. Law Rev. 75 (1), 109–135.

Berendt, B., Günther, O., Spiekermann, S., 2005. Privacy in e-commerce: stated preferences vs. actual behavior. Commun. ACM 48 (4), 101–106.

Boritz, J.E., No, W.G., 2011. E-commerce and privacy: exploring what we know and opportunities for future discovery. J. Inf. Syst. 25 (2), 11–45.

Boyatzis, R.E., 1998. Transforming Qualitative Information: Thematic Analysis and Code Development. Sage, Thousand Oaks, CA.

Braun, V., Clarke, V., 2006. Using thematic analysis in psychology. Qual. Res. Psychol. 3 (2), 77–101.

Brough, A.R., Martin, K.D., 2019. Critical roles of knowledge and motivation in privacy research. Curr. Opin. Psychol. 31, 11–15.

Campbell, C.R., Martinko, M.J., 1998. An integrative attributional perspective of empowerment and learned helplessness: a multimethod field study. J. Manag. 24 (2), 173–200.

Choi, H., Park, J., Jung, Y., 2018. The role of privacy fatigue in online privacy behavior. Comput. Hum. Behav. 81, 42–51.

Creswell, J.W., 2013. Research Design: Qualitative, Quantitative, and Mixed Methods Approaches, fourth ed. Sage Publications, Thousand Oaks, CA.

Culnan, M.J., Armstrong, P.K., 1999. Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation. Organ. Sci. 10 (1), 104–115.

Culnan, M.J., Bies, R.J., 2003. Consumer privacy: balancing economic and justice considerations. J. Soc. Issues 59 (2), 323–342.

Darke, P.R., Brady, M.K., Benedicktus, R.L., Wilson, A.E., 2016. Feeling close from Afar: the role of psychological distance in offsetting distrust in unfamiliar online retailers. J. Retail. 92, 287–299.

Debatin, B., Lovejoy, J.P., Horn, A., Hughes, B.N., 2009. Facebook and online privacy: attitudes, behaviors, and unintended consequences. J. Comput. Commun. 15 (1), 83–108.

Dienlin, T., Trepte, S., 2015. Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. Eur. J. Soc. Psychol. 45 (3), 285–297.

Dinev, T., 2014. Why would we care about privacy? Eur. J. Inf. Syst. 23 (2), 97–102.

Dinev, T., McConnell, A.R., Smith, H.J., 2015. Research commentary—informing privacy research through information systems, psychology, and behavioral economics: thinking outside the "APCO" box. Inf. Syst. Res. 26, 639–655.

Ellison, N.B., Vitak, J., Steinfield, C., Gray, R., Lampe, C., 2011. Negotiating privacy concerns and social capital needs in a social media environment. In: Trepte, S., Reinecke, L. (Eds.), Privacy Online. Springer, Berlin, Heidelberg, pp. 19–32. https://doi.org/10.1007/978-3-642-21521-6_3.

Eyal, T., Liberman, N., 2012. Morality and psychological distance: a construal level theory perspective. In: Mikulincer, M., Shaver, P. (Eds.), The Social Psychology of Morality: Exploring the Causes of Good and Evil. American Psychological Association, Washington DC, pp. 185–202.

Fereday, J., Muir-Cochrane, E., 2006. Demonstrating rigor using thematic analysis: a hybrid approach of inductive and deductive coding and theme development. Int. J. Qual. Methods 5 (1), 80–92.

Fransi, E.C., Viadiu, F.M., 2007. A study of e-retailing management: analysing the expectations and perceptions of Spanish consumers. Int. J. Consum. Stud. 31, 613–622.

Fujita, K., Henderson, M.D., Eng, J., Trope, Y., Liberman, N., 2006. Spatial distance and mental construal of social events. Psychol. Sci. 17 (4), 278–282.

Gerber, N., Gerber, P., Volkamer, M., 2018. Explaining the privacy paradox: a systematic review of literature investigating privacy attitude and behavior. Comput. Secur. 77, 226–261.

Guest, G., Bunce, A., Johnson, L., 2006. How many interviews are enough? An experiment with data saturation and variability. Field Methods 18 (1), 59–82.

Hallam, C., Zanella, G., 2017. Online self-disclosure: the privacy paradox explained as a temporally discounted balance between concerns and rewards. Comput. Hum. Behav. 68, 217–227.

Hartley, N., Green, T., 2017. Consumer construal of separation in virtual services. J. Serv. Theory Pract. 27, 358–383.

Holtrop, N., Wieringa, J.E., Gijsenberg, M.J., Verhoef, P.C., 2017. No future without the past? Predicting churn in the face of customer privacy. Int. J. Res. Mark. 34, 154–172.

Kim, K., 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. J. Interact. Mark. 25 (3), 145–158.

Kim, D.H., Sung, Y.H., Lee, S.Y., Choi, D., Sung, Y., 2016. Are you on Timeline or News Feed? The roles of Facebook pages and construal level in increasing ad effectiveness. Comput. Hum. Behav. 57, 312–320.

Kokolakis, S., 2017. Privacy attitudes and privacy behaviour: a review of current research on the privacy paradox phenomenon. Comput. Secur. 64, 122–134.

Lee, N., Kwon, O., 2015. A privacy-aware feature selection method for solving the personalization–privacy paradox in mobile wellness healthcare services. Expert Syst. Appl. 42 (5), 2764–2771.

Li, H., Luo, X.R., Zhang, J., Xu, H., 2017. Resolving the privacy paradox: toward a cognitive appraisal and emotion approach to online privacy behaviors. Inf. Manag. 54, 1012–1022.

Liberman, N., Trope, Y., 2008. The psychology of transcending the here and now. Science 322 (5905), 1201–1205.

Liberman, N., Trope, Y., Stephan, E., 2007. Psychological distance. In: Kruglanski, A.W., Higgins, E.T. (Eds.), Social Psychology: Handbook of Basic Principles. Guilford Press, New York, pp. 353–383.

Lincoln, Y.S., Guba, E.G., 1985. Naturalistic Inquiry. Sage, Beverly Hills.

Liviatan, I., Trope, Y., Liberman, N., 2008. Interpersonal similarity as a social distance dimension: implications for perception of others' actions. J. Exp. Soc. Psychol. 44 (5), 1256–1269.
Maier, S.F., Seligman, M.E., 1976. Learned helplessness: theory and evidence. J. Exp. Psychol. Gen. 105 (1), 3–46.
Martin, K., 2016a. Data aggregators, consumer data, and responsibility online: who is tracking consumers online and should they stop? Inf. Soc. 32 (1), 51–63.
Martin, K., 2016b. Understanding privacy online: development of a social contract approach to privacy. J. Bus. Ethics 137 (3), 551–569.
Martin, K., Nissenbaum, H., 2016. Measuring privacy: an empirical test using context to expose confounding variables. Columbia Sci. & Technol. Law Rev. 18, 176–218.
Martin, K.D., Murphy, P.E., 2017. The role of data privacy in marketing. J. Acad. Mark. Sci. 45 (2), 135–155.
Martinko, M.J., Gardner, W.L., 1982. Learned helplessness: an alternative explanation for performance deficits. Acad. Manag. Rev. 7 (2), 195–204.
McShane, L., Sabadoz, C., 2015. Rethinking the concept of consumer empowerment: recognizing consumers as citizens. Int. J. Consum. Stud. 39 (5), 544–551.
Merriam, S.B., Tisdell, E.J., 2016. Qualitative Research: A Guide to Design and Implementation, fourth ed. John Wiley & Sons, San Francisco, CA.
Norberg, P.A., Horne, D.R., Horne, D.A., 2007. The privacy paradox: personal information disclosure intentions versus behaviors. J. Consum. Aff. 41 (1), 100–126.
Novak, T.P., Hoffman, D.L., 2008. The fit of thinking style and situation: new measures of situation-specific experiential and rational cognition. J. Consum. Res. 36 (1), 56–72.
Pappas, I.O., 2018. User experience in personalized online shopping: a fuzzy-set analysis. Eur. J. Market. 52, 1679–1703.
Perkins, D.D., Zimmerman, M.A., 1995. Empowerment theory, research, and application. Am. J. Community Psychol. 23 (5), 569–579.
Petrescu, M., Krishen, A.S., 2018. Analyzing the analytics: data privacy concerns. J. Mark. Anal. 6 (2), 41–43.
Saunders, M., Lewis, P., Thornhill, A., 2012. Research Methods for Business Students, sixth ed. Pearson Education, Essex, UK.
Schneider, M.J., Jagpal, S., Gupta, S., Li, S., Yu, Y., 2017. Protecting customer privacy when marketing with second-party data. Int. J. Res. Mark. 34 (3), 593–603.
Silverman, D., 2011. Interpreting Qualitative Data: A Guide to the Principles of Qualitative Research, fourth ed. Sage, London.
Simon, H.A., 1982. Models of Bounded Rationality: Empirically Grounded Economic Reason. MIT Press, Cambridge, MA.
Simon, H.A., 1955. A behavioral model of rational choice. Q. J. Econ. 69 (1), 99–118.
Smith, H.J., Dinev, T., Xu, H., 2011. Information privacy research: an interdisciplinary review. MIS Q. 35, 989–1016.
Sofaer, S., 1999. Qualitative methods: what are they and why use them? Health Serv. Res. 34 (5 Pt 2), 1101–1118.
Spreitzer, G.M., 1995. Psychological empowerment in the workplace: dimensions, measurement, and validation. Acad. Manag. J. 38 (5), 1442–1465.
Statista, 2018a. Desktop retail e-commerce sales in the United States from 2002 to 2017. https://www.statista.com/statistics/273424/retail-e-commerce-sales-in-the-united-states/, Accessed date: 12 May 2019.
Statista, 2018b. Number of Digital Buyers Worldwide from 2014 to 2021. https://www.statista.com/statistics/251666/number-of-digital-buyers-worldwide/, Accessed date: 12 May 2019.
Strauss, A., Corbin, J., 1998. Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory. Sage, Newbury Park, CA.
Taddei, S., Contena, B., 2013. Privacy, trust and control: which relationships with online self-disclosure? Comput. Hum. Behav. 29 (3), 821–826.
Tene, O., Polonetsky, J., 2012. Big data for all: privacy and user control in the age of analytics. Northwest. J. Technol. Intellect. Prop. 11 (5), 239–273.
Terpstra, A., Schouten, A.P., de Rooij, A., Leenes, R.E., 2019. Improving privacy choice through design: how designing for reflection could support privacy self-management. Clin. Hemorheol. and Microcirc. 24 (7). https://firstmonday.org/ojs/index.php/fm/article/view/9358/8051.
Trope, Y., Liberman, N., 2010. Construal-level theory of psychological distance. Psychol. Rev. 117 (2), 440–463.
van Dyke, T., Midha, V., Nemati, H., 2007. The effect of consumer privacy empowerment on trust and privacy concerns in e-commerce. Electron. Mark. 17 (1), 68–81.
Wakslak, C.J., Trope, Y., Liberman, N., Alony, R., 2006. Seeing the forest when entry is unlikely: probability and the mental representation of events. J. Exp. Psychol. Gen. 135 (4), 641–653.
Wieringa, J., Kannan, P.K., Ma, X., Reutterer, T., Risselada, H., Skiera, B., 2019. Data analytics in a privacy-concerned world. J. Bus. Res. https://doi.org/10.1016/j.jbusres.2019.05.005.
Zafeiropoulou, A.M., Millard, D.E., Webber, C., O'Hara, K., 2013. Unpicking the privacy paradox: can structuration theory help to explain location-based privacy decisions? In: Proceedings of the 5th Annual ACM Web Science Conference, pp. 463–472 Paris, France.
Zimmerman, M.A., 1995. Psychological empowerment: issues and illustrations. Am. J. Community Psychol. 23 (5), 581–599.