THE ROLE OF CONSUMER KNOWLEDGE IN THE PRIVACY PARADOX OF PERSONALISED ADVERTISING

Miralem Zahirović, Esmeralda Marić, Melika Husić-Mehmedović

Abstract

Current literature on the privacy paradox in personalised advertising lacks insight into how consumers' knowledge of the data types used shapes their responses to these ads. Building on privacy calculus theory, theory of reasoned action, and signalling theory, this research explores how consumers' knowledge of data types in personalised advertising influences their reactions. Multigroup path analysis examines differences in established relationships based on consumers' data knowledge. The moderating effect of this knowledge in the relationship between perceived invasiveness and purchase intentions is also tested. Findings from a sample of millennials indicate that privacy concerns increase perceived invasiveness. However, multigroup and moderation analyses reveal that perceived invasiveness' impact on purchase intentions varies with consumers' data knowledge. Specifically, in the search history group, perceived intrusiveness negatively affects purchase intentions. These results underscore the situation-specific nature of the privacy calculus and assist advertisers in understanding consumer behaviour in response to personalised ads.

Miralem Zahirović, MA
Country: Bosnia and Herzegovina
E-mail: miralem.zahirovic@yahoo.com

Esmeralda Marić, MA
Title: Teaching assistant
Institution: School of Economics and Business,
University of Sarajevo
Country: Bosnia and Herzegovina
E-mail: esmeralda.maric@efsa.unsa.ba
ORCID: 0000-0003-4959-3735

Melika Husić-Mehmedović, PhD
Title: Full Professor
(Corresponding author)
Institution: School of Economics and Business,
University of Sarajevo
Address: Trg oslobođenja – Alija Izetbegović 1,
71000 Sarajevo
Country: Bosnia and Herzegovina
E-mail: melika.husic@efsa.unsa.ba
ORCID: 0000-0002-0802-2752

1. INTRODUCTION

Personalised advertising is a growing trend in online advertising (Brinson and Eastin 2016; Tucker 2014). In recent years, online advertising has become highly personalised, with content tailored to the needs of consumers. Personalisation has many benefits, but the preference for personalised experiences comes at a price. Consumers perceive personalised advertising as a valuable time-saving tool, and it is widely accepted

(Lee, Im, and Taylor 2008; Srinivasan, Anderson, and Ponnavolu 2002). The main problem in personalised advertising is that high invasiveness impairs purchase intentions (Phelps, D'Souza, and Novak 2001). Personal information collected without knowledge and consent leads to a negative attitude towards this practice (Xu, Dinev, Smith, and Hart 2011). The growing number of invasive advertisements leads to greater concerns among consumers, resulting in the need for a secure online environment (Tucker 2014).

Many recent research efforts have focused on understanding the effects of risks and benefits associated with personalised advertising on attitudes (Taylor, Lewin, and Strutton 2011) and behavioural intentions (Baek and Morimoto 2012; Lin and Kim 2016). These studies often provide contradictory results that make further research on this topic imperative. Considering that recent research on advertising signals suggests a dual nature of the information cues conveyed (Taj 2016), a more detailed investigation of the universality of relationships in a risk-related side of privacy calculus in personalised advertising as a function of consumers' knowledge of the data types used for personalised advertising is needed. Offering quite conflicting results on the effectiveness of personalised advertising, the literature lacks a comprehensive understanding of the role that situational factors, such as consumer knowledge of the data types used in personalised ads, play in shaping purchasing decisions. This research draws on the privacy calculus theory, the theory of reasoned action and the signalling theory. It aims to analyse the risk-related side of the privacy calculus theory and explore if established relationships in the risk-related side of the privacy calculus theory differ across consumers with different knowledge of the data types used. Specifically, as the analysis proceeds, we explore if consumer knowledge of the data types used in personalised advertising creates differences in their purchase intentions upon perceiving the invasiveness of personalised ads. For the purpose of achieving this aim, this research relies on a similar, multigroup analysis-based procedure to a study by Gironda and Korgaonkar (2018) and complements it with a moderation analysis. By exploring what is previously explained, this research contributes to the theory in two different ways. First, it explores the universality of the risk-related side of the privacy

calculus across consumers with different knowledge of the data types used for personalised advertising using a multigroup analysis approach. Second, it explains how this situational factor changes established relationships. Furthermore, the research has important implications for business management as it explains customer behaviour in an online environment and sheds light on the importance of educating and informing consumers about personalised advertising.

The following text included a thorough literature review on personalised advertising and the privacy calculus theory. We then develop our hypothesis and research question and proceed with the methodology explanations and result presentation. Finally, we provide a detailed discussion of our findings, state the limitations of our research and offer recommendations for future researchers.

2. LITERATURE REVIEW

2.1. Personalised Advertising

In terms of personalised advertising, personalisation means that elements about the target customers are integrated into the text of an ad (Dijkstra and Ballast 2012). The concept of personalisation is narrower than customised (tailored) communication, as the latter is an umbrella term for personalisation, feedback, contextual adaptation, source matching and consumer exposure (Dijkstra 2008). Data segmentation plays a crucial role in creating personalised ads.

Companies use data segmentation to improve the relevance of advertising, reduce the risk of irritation and increase the effectiveness of personalised advertising (Gironda and Korgaonkar 2018). However, various studies have found that consumers have negative attitudes towards personalised advertising and that these attitudes often do not depend on factors such as time, level of education regarding digital tracking practices and the use of advanced advertising technology (e.g. Aguirr et al. 2015; Boerman, Kruikemeier, and Bol 2021; Bol et al. 2018; Frick and Li 2016; Karwatzki, Dytynko, and Veit 2017; Matic et al. 2017; White et al. 2008;). Consumers who are informed about data collection, dissemination, and potential use of personal data make some technological and non-technological efforts to protect themselves from potential risks (Li

and Nill 2020). Nevertheless, consumption of personalised content includes the trade-off between benefits and risks, which is all a matter of concern in the privacy calculus.

2.2. The privacy calculus theory

The privacy calculus model can be explained as the relationship between the expected benefit and the perceived risk in terms of consumer privacy. Knijnenburg et al. (2017) discuss the descriptive and prescriptive aspects of the model. Under the descriptive aspect, the privacy calculus is based on the premise that consumers use a rational cognitive process to evaluate the risks and benefits of disclosing personal information. The concept of privacy is defined differently in the literature (Boerman and Smith 2023). Taking the Internet as an example (Dinev et al. 2013), privacy is presented as a broad and fragmented concept of information privacy. According to one of the generally accepted classifications of privacy (Burgoon 1982), information privacy is characterised as the ability to control the collection and dissemination of information. The fundamental characteristic of the Internet is that users leave permanent traces, which is considered the basic principle of online privacy. Since information and privacy are seen as consumer goods, consumers must decide whether to disclose personal information in exchange for a benefit by weighing the perceived risk and expected benefit. This again points to the premise of the model that the decision to disclose information is a rational process. On the other side, the prescriptive version of the privacy calculus model, on the other hand, favours a contextual approach. This adaptive (contextual) approach refers to the transfer of responsibility for decision-making from consumers to an algorithm that takes into account a number of elements — context, consumer characteristics and the history of consumer decisions of similar profiles.

The following discussion focuses on the descriptive aspect of the privacy calculus theory, explaining two opposite elements of the privacy calculus: the relevance of personalised advertising as the benefit-related side of the privacy calculus theory and privacy concerns as the risk-related side of the privacy calculus theory.

2.3. Relevance of Personalised Advertising and Privacy Concerns

The relevance of personalised advertising means that the content of the advertising corresponds to the interests and needs of the consumers. If the advertised product has a certain value to the consumer, some of this value will also be transferred to the advertisement, resulting in greater relevance (Xu and Zhou 2013). The value of advertising is subjective and depends on information, deception, irritation, and entertainment factors (Ducoffe 1995). Consumers consciously choose to interact with advertising and invest their time. As they expect highly relevant advertising, they agree that companies collect and use their personal information.

However, in addition to the relevance of personalised advertising, privacy concerns play an important role in shaping consumer responses to personalised ads. Loss of control increases privacy concerns (Piao et al. 2016; Tucker 2014), which can block desired business outcomes (Hoffman, Novak, and Peralta 1998; McKnight and Chervany 2002; Urban et al. 2009). Furthermore, empirically validated conclusions suggest that privacy concerns decrease when consumers have more control over their personal information (Lee and Cranage 2011). In the privacy calculus model, the increase in perceived control over privacy can be seen as a benefit as it ultimately reduces privacy concerns and perceived invasiveness. A lot of factors can influence the formation of privacy concerns, and even artificial intelligence seems to be one of them (Kronemann et al. 2023).

2.4. The invasiveness and privacy paradox

The concept of invasiveness is difficult to separate from privacy concerns because this concept would not exist if consumers did not think about the practice of online tracking. Privacy concerns, then, mean that consumers are concerned about the practice of tracking resulting from individual development, environmental influences, and social interactions (Lwin and Williams 2003). Considering that the environment and experiences shape an individual's attitude, the perceived invasiveness of advertising based on

personalisation can be described as a belief in a clear violation of online privacy from the consumer's perspective (Wieczorkowski and Polak 2017).

The privacy paradox is inherent in the privacy calculus model, which is based on the premise that the risk-benefit assessment of personal information disclosure is a rational cognitive process (Knijnenburg et al. 2017). According to the privacy calculus, consumers strive to maximise benefits and minimise risk. Information asymmetry is the most common cause of the privacy paradox (Wilson and Valacich 2012). As a result of information asymmetry, uninformed consumers rely on heuristic methods when making decisions (Dietrich 2010). The more consumers are informed about protection strategies, the higher the risk perception (Gironda and Korgaonkar 2018), but practice has shown that this is not a sufficient reason for implementing avoidance strategies. Most importantly, situational factors can impair established relationships in the privacy calculus, resulting in consumer reactions that are different from what could be expected.

3. HYPOTHESIS DEVELOPMENT

Concerns about the protection of privacy through personalised advertising are often linked to negative consequences for behaviour. According to privacy calculus theory, the risk associated with disclosing personal information has a negative effect on behaviour, and the final decision about behaviour is made through a rational risk-benefit calculation (Culnan and Armstrong 1999). However, most of the previous efforts have been aimed at understanding the effect of privacy concerns on ad reactance. These studies proved the positive effect of privacy concerns on ad avoidance (Beak and Morimoto 2012; Ham 2017) and their negative effect on the intention to share an ad (Lee, Kim, and Ham 2016). In addition, research has shown that higher levels of privacy concerns lead to lower levels of information disclosure (Li, Cho and Goh 2019) and increased privacy measures (Miltgen, Cases, and Russel 2018). The effect of privacy concerns on purchase intention has rarely been studied compared to efforts to measure the impact on advertising-related behavioural consequences. However, it has been reported that purchase intent decreases due to

greater privacy concerns with personalised advertising (Lin and Kim 2016). In addition, researchers have demonstrated that the higher perceived risks associated with disclosing personal information lead to a lower intention to share personal information, which in turn has a positive impact on purchase intentions related to location-based mobile advertising (Kurtz, Wirtz, and Langer 2021). Interestingly, in a study based on the theory of reasoned action (TRA) (Ajzen and Fishbein 1980), according to which beliefs regarding a certain action influence attitudes toward that action and, through attitudes, behavioural intentions and behaviour, the technology acceptance model (TAM) was applied to assess the effects of Facebook ad privacy concerns as behavioural beliefs on behavioural intentions (Lin and Kim 2016). The results showed a significant negative effect of such beliefs on purchase intention. Based on privacy calculus theory, the theory of reasoned action, and the available literature, we propose:

H1: Privacy concerns in the context of personalised advertising negatively affect purchase intentions.

Various studies have shown that privacy concerns related to personal advertising have both cognitive and behavioural effects. Among the most common cognitive consequences of privacy concerns, researchers include intrusiveness or invasiveness (Beak and Morimato 2012; Van Doorn and Hoekstra 2013; Morimoto 2021; Mpinganjira and Maduku 2019). When people feel that an ad is too personal, they react to it (White et al. 2008) and have a strong sense of abuse (Okazaki, Li, and Hirose 2009) because they cannot control their personal information. Some authors see intrusiveness as a facet of invasiveness and define it as the realisation that private information is being used for advertising without their knowledge (Morimoto 2017). Invasiveness in itself is the extent to which consumers feel that advertising invades their privacy and creates a sense of loss of control over the information they consider their own (Miltgen, Cases, and Russel 2019) and is directly related to privacy concerns that exist in the age of online networks and social media (Gironda and Korgaonkar 2018; Sheehan and Hoy 1999). Since there appears to be a strong connection between personalisation and invasiveness (Taylor, Lewin, and Strutton 2011) and evidence that consumers tend to experience a sense of invasion

when their data is used without them being aware of this use, we suggest that consumers exhibiting high privacy concerns should record higher levels of invasiveness when exposed to personalised ads. Therefore, we hypothesise:

H2: Privacy concerns positively affect the perceived invasiveness of personalised advertising.

Previous research suggests that the perception of the practice as something that violates privacy (Paschal et al. 2009) negatively influences behavioural intentions in various contexts (Gironda and Korgaonkar 2018; Thibodeaux and Kudisch 2003). Gironda and Korgaonkar (2018) conducted one of the first studies on the effects of intrusiveness on behavioural intentions in terms of engagement (intention to click) and purchase intention. Their results show a significant relationship in both paths, suggesting the accuracy of the risk-related side of privacy calculus theory in the context of personalised advertising. Following the logic of the privacy calculus theory and the available literature, we propose the following:

H3: Perceived invasiveness of personalised advertising negatively affects purchase intentions.

3.1. The privacy calculus theory, information asymmetry, and information signalling

Privacy calculus is conceptualised as a highly situation-specific trade-off (Kehr, Wentzel, and Mayer 2013; Kehr et al. 2015). The company-consumer relationship is characterised by high information asymmetry (Sun, Wang, and Shen 2021). When it comes to personalised advertising on social media, consumers cannot always assess which information related to their characteristics or online behaviour is used to create personalised ads, which harms information asymmetry (Wang et al. 2020). The asymmetry is reduced when educated consumers know something about the data used. However, we still don't know with certainty if the relationships between perceived risks and behavioural responses are under the influence of the consumers' knowledge. Different types of information and their quantity can be one of the situational factors that may, but not necessarily, lead to differences in previously hypothesised relationships (Gironda and Koragankar 2018). Following recent findings on the signalling theory in organisational communication (Taj 2016), it's important to acknowledge that the information on the data types implies more than fear or risk and could potentially be used to assess relevance and create changes in established relationships in the risk-related side of the privacy calculus. Therefore, we raise the following research question:

RQ1: Do the proposed relationships between privacy concerns, perceived invasiveness, and purchase intentions in personalised advertising differ depending on consumers' knowledge of the data types used for personalised advertising and how?

Figure 1. Conceptual model
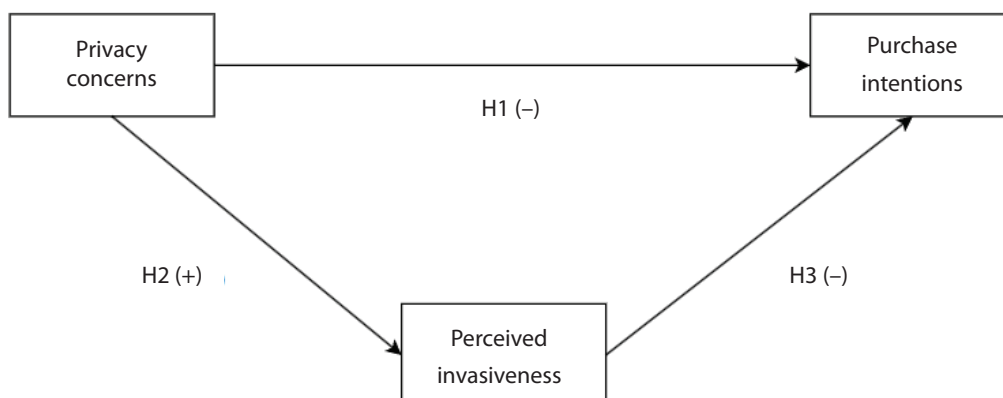
4. METHODOLOGY

The main goal of this research is to determine how situational factors in terms of consumer knowledge of data used for the creation of personalised ads affect their responses to these ads. Specifically, we wanted to test the universality of established relationships in the risk-related side of the privacy calculus across consumers with different knowledge of the data type used for personalised advertising and explore how consumer knowledge creates differences in these relationships.

4.1. Research design

We designed a quasi-experimental research to test our hypothesis and answer our research question. The research instrument is a questionnaire based on scenarios. Respondents were randomly assigned a questionnaire with a scenario guaranteeing data privacy and anonymity. Scenarios were used to examine the possible discrepancy in our hypothesised relationships caused by the respondents' knowledge about the data used for personal advertisements. A control group was part of the first sub-sample, and the scenario generally describes the practice of personalised advertising without mentioning the type of data used for advertising. Besides general information about ads using personalisation, the second scenario encompassed a situation in which personalised advertising was created as a result of search history. Finally, the third group received the scenario in which, in addition to the general description of personal advertising, the use of metadata for such an advertisement was mentioned. In this third scenario, a general classification of metadata was provided; we told research participants that a diverse group of data, such as search history, social media posts, email, etc., was used to create such an advertisement. Using these three scenarios was essential for testing the applicability and universality of our model. Since it was previously mentioned that the impact of the risk-related factors of the privacy calculus theory on purchase intentions could be different depending on situational circumstances, these three scenarios represent three different situations across which we wanted to test our hypothesised paths and check for their universality.

4.2. Sample and Instrument

This research relies on the convenience sampling method. Data was collected at the beginning of 2022, and the sample included 300 millennials. According to the gender structure, the ratio of respondents was approximately the same, with the male respondents representing 51.3% of our sample. The respondents belong predominantly to the millennial generation born between 1980 and 1996. Most of our research participants had a university degree, 192 of them, or 64%. They were followed by respondents with acquired high school diplomas (21.3%) and masters (13.7%). According to the structure of employment, respondents who are employed full-time form the largest group, which makes up 80.3% of our sample.

The questionnaire included four questions on demographics, followed by questions from the scales we used. Privacy concerns were measured using the Internet Privacy Concerns scale (Dinev and Hart 2006). The perception of invasiveness was measured using the Invasiveness Perceptions scale (Tepper and Braun 1995), while purchase intentions were measured through the Behavioral Intention scale (Venkatesh et al. 2003).

5. EMPIRICAL ANALYSIS

Following an established multigroup structural equation modelling procedure, we started our analysis by testing measurement invariance through multigroup confirmatory factor analysis (MGCFA) (Steenkamp and Baumgartner 1998). Three types of invariances are assessed: configural, metric, and factor covariance invariance. Since all indices indicated a very good model fit of our multigroup CFA according to widely applied thresholds (Bentler and Bonett 1980; Hu and Bentler 1999; Steiger 2007; Tabachnick and Fidell 2007), configural invariance was supported. By constraining factor loading to equality, we assessed metric invariance, after which we tested factor covariance invariance. Reflecting on good model fits of newly established models and insignificant change in the chi-square tests, our analysis supported metric invariance and factor covariance invariance. These results indicate that our constructs have the same meaning across the groups and that the relationships

among study constructs can be compared across our experimental groups. However, it is worth mentioning that we removed one item from the original Privacy Concerns scale due to bad model fit, which is a common practice (i.e., Zhao and Othman 2011). A possible explanation for the worse fit with the item included might be the sample size, and in that case, measurement item purification is acceptable (Hair et al. 2006). Our multigroup CFAs remaining within-group standardised loadings were all above 0.6, respectively (Awang 2014). The results of invariance testing and multigroup CFA are in Tables 2 and 3.

The results from multigroup CFA were used to test discriminant and convergent validity for each group. Since average variance extracted (AVE) values were above 0.5, the squared root of AVE for each construct proved to be higher than correlations between latent variables (Fornell and Larcker 1981), composite reliability was above 0.7, and item standardised loadings were higher than 0.6, we can conclude that convergent and discriminatory validity are supported (Table 2). Each model had a satisfactory model fit: No data group (χ^2=24.148, RMSEA=0.008, SRMR=0.042, GFI=0.950, CFI=1), Search history group (χ^2=44.606, RMSEA=0.093, SRMR=0.056, GFI=0.915, CFI=0.970), and Metadata group (χ^2=45.729, RMSEA=0.088, SRMR=0.047, GFI=0.916, CFI=0.969). The presented results are above-accepted thresholds in the literature of 0.95 for CFI (Hu and Bentler 1999), 0.9 for GFI (Shevlin and Miles 1998), below 0.08 for SRMR (Hu and Bentler 1999), and 0.1 for RMSEA (Fabrigar et al. 1999). For the second and third experimental groups, it's worth mentioning that RMSEA above the cutoff of 0.08, when accompanied with values of other indices indicating good fit can be expected due to lower sample size, and evaluation of such model solely based on RMSEA could lead to rejection of such model, even though it is correctly specified (Kline 2015). In

Table 1. Invariance testing

Model	χ^2	df	$\Delta\chi^2$	Δdf	p-value ($\Delta\chi^2$, Δdf)	RMSEA	NFI	CFI	AIC
Unconstrained	114.883	74	-	-	-	0.043	0.942	0.978	236.483
Measurement weights	132.317	86	17.434	12	0.121	0.043	0.933	0.975	230.317
Structural covariances	144.46	98	29.577	24	0.185	0.040	0.926	0.975	218.460

Table 2. Factor loadings, composite reliability, and correlations

Constructs	Loadings	CR	1	2	3
No data information					
1. Privacy Concerns	(0.845-0.927)	0.951	**0.930**		
2. Perceived Invasiveness	(0.799-0.890)	0.932	0.630	**0.903**	
3. Purchase Intentions	(0.665-0.913)	0.901	-0.221	-0.159	**0.869**
Search history					
1. Privacy Concerns	(0.889-923)	0.962	**0.827**		
2. Perceived Invasiveness	(0.813-0.929)	0.855	0.781	**0.925**	
3. Purchase Intentions	(0.747-0.942)	0.824	-0.173	-0.256	**0.908**
Metadata					
1. Privacy Concerns	(0.903-0.928)	0.970	**0.923**		
2. Perceived Invasiveness	(0.749-0.883)	0.919	0.739	**0.889**	
3. Purchase Intentions	(0.789-0.928)	0.912	0.024	-0.056	**0.945**

Notes: CR=Composite Reliability, squared roots of AVE (Average Variance Extracted) are on the diagonal line, and correlations are below the line

the case of the first experimental group, our model fits almost perfectly, with the Chi-square value being insignificant.

After finalising the MGCFA analysis, we proceeded to path analysis for hypothesis testing. By observing our results, we can conclude that privacy concerns have a strong positive impact on perceived invasiveness in all of our experimental conditions ($\beta_{\text{No data}}$ = 0.648, p < 0.000; $\beta_{\text{Search history data}}$= 0.774, p < 0.000; β_{Metadata} = 0.749, p < 0.001), which confirms

our hypothesis H1. However, Privacy concerns don't significantly affect Purchase intention in any of our groups. Interestingly, unlike in the case of the other two groups, in the case of the Search history data group, perceived invasiveness significantly affects Purchase intention (β = -0.317, p < 0.05). None of our control variables (birth year (age) and gender) have a significant impact on endogenous variables in our model (perceived invasiveness and Purchase Intention), considering two-tailed p values.

Table 3. Path analysis

Paths	No data information	Search history	Metadata
H1: Privacy concerns → Perceived Invasiveness	0.648***	0.774***	0.749***
H2: Perceived Invasiveness → Purchase Intention	-0.037	-0.317*	-0.158
H3: Privacy concerns → Purchase Intention	-0.202	0.090	0.111
Controls:			
Birth year (Age) → Perceived Invasiveness	0.109	-0.047	0.012
Birth year (Age) → Purchase Intention	-0.009	-0.131	0.076
Gender → Perceived Invasiveness	0.141	0.107	-0.093
Gender → Purchase Intention	0.04	-0.038	-0.197
R^2	0.422	0.622	0.558

Global model fit: χ^2=135.138, df=108, χ^2/df=1.251, RMSEA=0.029, NFI=0.933, CFI=0.985

Note: *** p one-tailed significant at 0.1% level, * p one-tailed significant at 5% level

Figure 2. Moderation effect of consumers' knowledge of the data used for personal advertising
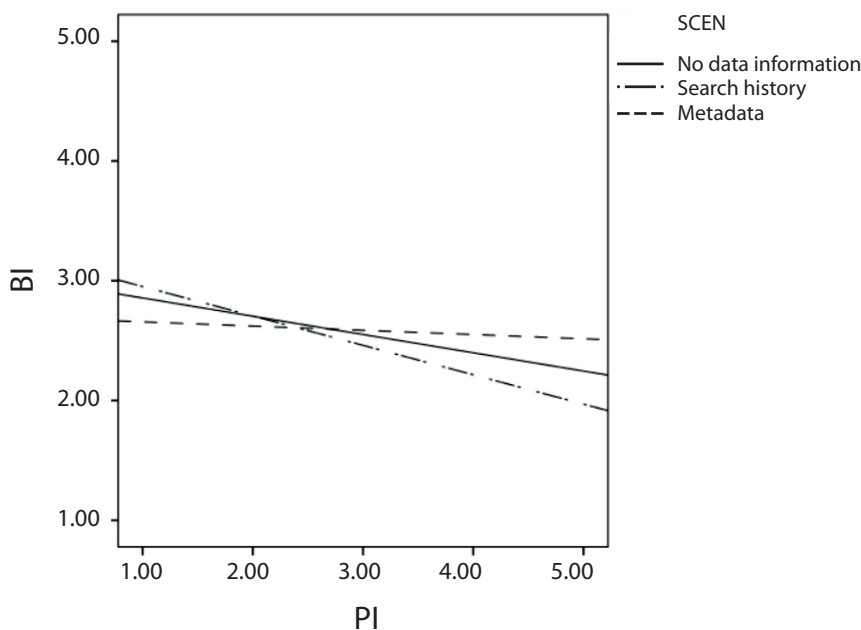
Note: BI (purchase intention), PI (perceived invasiveness)

Since our analysis indicated differences in the relationship between perceived invasiveness and purchase intention between our three experimental groups, we proceeded with moderation analysis in Process, Model 1 (Hayes 2017). In the model specification, experimental groups that represented information on the data used were used as a multicategorical moderator. Our results show that our experimental groups (information on data used for personal advertising) serve as a significant moderator of the relationship between perceived invasiveness and purchase intention, with the effect for Perceived invasiveness*Search history data being -0.246 ($p <$ 0.05, LLCI = -0.457, ULCI = -0.0339), which can be clearly observed from Figure 2.

6. DISCUSSION AND CONLUSIONS

The aim of this research was to examine the generalizability of the relationship between privacy concerns regarding personalised advertising, perceived invasiveness and purchase intentions across consumers with different knowledge of data types used in personalised advertising and explore the moderating effects of the consumer knowledge of data types used in personalised advertising in the relationship between perceived intrusiveness and purchase intentions.

As expected, privacy concerns increase perceived invasiveness. However, the direct effect of privacy concerns on purchase intentions is lacking, which draws some attention to the benefit-related side of the privacy calculus. Previous studies confirm that consumers perform a risk-benefit calculation of all factors when evaluating privacy concerns (Culnan and Armstrong 1999). They are even willing to disclose more personal information if the perceived benefit of personalised advertising is higher (Bol et al. 2018). They are aware that their behaviour is being monitored and that their private information is being used (Montgomery et al. 2019). Although this awareness may increase privacy concerns, this may not be reflected in reduced purchase intentions as consumers are used to personalised advertising and have had positive experiences with it because they are advertised with products and services that meet their personal needs (Meyer and Schwager 2007). This brings us to the utilitarian side of the privacy calculus theory, which leads us to believe that the benefits of personalised advertising outweigh the disadvantages in decision-making (Taddicken 2014).

Our research shows that the effect of invasiveness on purchase intent depends on whether consumers know what data types are used for personalised advertising. Although the conclusion on the effects of privacy concerns on purchase intentions and perceived invasiveness is the same across groups of consumers with different knowledge of the type of data used in personalised advertising, differences between groups occur in the relationship between perceived invasiveness and purchase intentions, leading us to a conclusion that situational factors in terms of the type of data used for personalised ads indeed plays an important role in shaping consumer responses. An insignificant effect is observed in the relationship between perceived invasiveness and purchase intentions in the group without data information and the group with metadata. However, the significant negative effect of perceived invasiveness on behavioural intentions is present in the case of the group with search history, which contradicts some previous findings suggesting significant relationships when more data is used (e.g., metadata) (Gironda and Korgaonkar 2018). To conduct a more thorough analysis, we tested the moderating effect of knowledge about the type of data used for personalised ads in the relationship between perceived invasiveness and purchase intention using Process Macro. The analysis proved the significance of the abovementioned moderating effect. The explanation for these results could again be based on the utility side of the privacy calculus model and ad relevance (Zhu and Chang 2016). Even when they perceive an ad as invasive, consumers' purchase intentions don't decrease when they rate the benefits of personalised advertising higher than the risks associated with the use of their personal information (Desimpelaere, Hudders, and Van de Sompel 2021). Personalised ads are more relevant; consumers are targeted based on their preferences, which saves them time (Srinivasan, Anderson, and Ponnavolu 2002). Moreover, it is not only the time-saving benefit that consumers experience. Receiving benefits such as customised service (Xu 2006), personalised entertainment (Lee, Im, and

Taylor 2008) and benefits related to their social image and self-perception as well as financial rewards (Lee, Ahn, and Bang 2011) can result in desired behavioural responses and prevent the negative effects of privacy-related risks on purchase intentions. When multiple types of information are used to create ads and consumers recognise this, they may consider the ads more relevant, so the perception of invasiveness does not lead to a significant decrease in purchase intention, which explains the non-significant effect in the case of the metadata group. The situation is similar for the metadata group: If they do not learn anything about the data, they may assume that a diverse information base was used, so the effect is also not significant. However, limiting and focusing cognitive focus solely on search history data can lead to consumers perceiving ads as irrelevant and not tailored to their needs. If consumers feel that not enough information is being used to create ads, their sense of invasion of privacy is sufficient to reduce purchase intention due to perceived lower relevance. This is consistent with previous research highlighting the prevailing effect of utility on behavioural intentions (Taddicken 2014) as well as the lower degree of creepiness and higher degree of relevance of unique personalised advertising among modern consumers (Eisend and Tarrahi 2022). All of this means that our findings represent an important addition to current knowledge about the situation-specific nature of the privacy calculus in the context of personalised advertising and provide a new perspective on information signalling and the privacy calculus through multigroup path analysis and moderation tests.

7. IMPLICATIONS, LIMITATIONS AND RECOMMENDATIONS

Our study has multiple theoretical and practical contributions. First of all, the study contributes theory on the risk-related side of the privacy calculus theory when applied to personalised advertising. The way this study contributed to the risk-related side of the privacy calculus in personalised advertising is by testing the generalizability of established relationships in this side of the privacy calculus across consumers with different knowledge of data types used for

personalised advertising and proving the moderating role of this knowledge in the relationship between perceived invasiveness and purchase intentions. This means that although increased privacy concerns increase perceived invasiveness, increased perceived invasiveness doesn't necessarily mean decreased purchase intentions. This finding is novel and unique in the literature because prior research tackling the role of consumer knowledge offers limited insights into how it changes established relationships. By doing so, our research draws some attention to the role of consumer knowledge of data used in personalised advertising and information signalling that should be even more explored.

From a practical perspective, this research helps online advertisers understand the purchasing behaviour of consumers exposed to personalised ads. Although privacy concerns play crucial roles in the legalisation part of personalised advertising, our research suggests that, from the perspective of the effectiveness of these ads, managers should pay a lot of attention to what consumers know about the data types used. These concrete findings, therefore, have significant implications for how online advertisers communicate and engage in the talk about data used for the creation of personalised ads. Educating consumers on data used for the creation of personalised ads is very important because our research proves that this knowledge is a crucial factor in moderating common relationships in the risk-related side of privacy calculus. Consumers learn about personalised advertising from various sources and having in mind that this knowledge changes relationships leading to their purchase intentions, advertisers should engage more in this process of education. For example, suppose they think consumers could assume that they used search history data to create personalised ads. In that case, they should make sure that they inform consumers about the usage of metadata for ad creations and its relevancy. In general, what consumers know about data types used for personalised advertising changes how they respond to invasive ads, and advertisers should be aware of it.

One of the limitations of our study is the reliance on a sample consisting of millennial consumers. Future research could include a more diverse demographic structure. However, the main limitation of

our study is the fact that we did not test the impact of the perceived usefulness of personalised advertising. The logic behind the privacy-calculus theory, from which we derive most of our explanations, has led us to assume that insignificant effects are observed due to benefits associated with the personalisation of advertising, i.e. relevance. However, it would also be beneficial to test the effects of perceived benefits on purchase intentions. As our study revealed some differences in the scenario comparisons compared to the study by Gironda and Korgankar (2018), we encourage future researchers to analyse the universality of the scenarios in different contexts. Since we draw explanations of our findings of the role of consumer knowledge of the type of data used from the prior research and theories about the information, future research should empirically test the relevance of the data information from our scenarios and examine the impact of this relevance on behavioural intentions. This would be a useful addition to our research as it would explain the mechanisms behind the impact of consumers' knowledge of the data used in the creation of personalised advertising on behavioural intentions. We have not hypothesised this, but it has emerged as a possible explanation for our findings when placed in the context of previous empirical research and relevant theories.

Future research should consider including online privacy protection and regulation issues, either as central themes or as moderating factors, to better understand the dynamics between privacy concerns, perceived invasiveness, and purchase intentions. This approach can provide a more comprehensive analysis of how regulatory environments influence consumer behaviour in digital contexts. In addition, further research on the specific situational factors is needed, as the effects of risks and benefits on behavioural intentions obviously depend on these situational factors. Future researchers could also focus on specific media of personalised advertising because recent research proves that consumer reactions to personalised ads might differ due to the ad source (De Keyzer, van Nort, and Kruikemeier 2022). Based on the above, we conclude that further research is needed to understand the mechanisms in the decision-making process that follows personalised advertising.

References

Aguirr, L. E., Mahr, F. D., Grewal, D., de Ruyter, J. C., and Wetzels, M. G. M. 2015. Unraveling the personalization paradox: The effect of information collection and trust-building strategies on online advertisement effectiveness. Journal of Retailing 91 (1): 34-49.

Ajzen, I., and Fishbein, M. 1980. Understanding attitudes and predicting social behavior. Englewood Cliffs, NJ: Prentice Hall.

Awang, Z. 2014. A Handbook of SEM for Academicians and Practitioners. The Step by Step Practical Guides for the Beginners, MPWS Rich Publication, Bangi

Baek, T. H., and Morimoto, M. 2012. Stay away from me. Journal of advertising 41 (1): 59-76.

Baek, T.H., and Morimoto, M. 2012. Stay away from Me: Examining the Determinants of Consumer Avoidance of Personalized Advertising. Journal of Advertising 41: 59-76.

Bentler, P.M. and Bonett, D.G. 1980. Significance tests and goodness of fit in the analysis of covariance structures. Psychological bulletin 88 (3): 588.

Boerman, S. C., and Smit, E. G. 2023. Advertising and privacy: an overview of past research and a research agenda. International Journal of Advertising 42 (1): 60-68.

Boerman, S., Kruikemeier, S., and Bol, N. 2021. When is personalized advertising crossing personal boundaries? How type of information, data sharing, and personalized pricing influence consumer perceptions of personalized advertising. Computers in Human Behavior Reports, 4.

Bol, N., Kruikemeier, S., Boerman, S., Strycharz, J., de Vreese, C, Dienlin, T., Sax, M., and Helberger, N. 2018. Understanding the Effects of Personalization as a Privacy Calculus: Analyzing Self-Disclosure Across Health, News, and Commerce Contexts. Journal of Computer-Mediated Communication 23 (6): 370-388.

Brinson, N. H., and Eastin, M. S. 2016. Juxtaposing the persuasion knowledge model and privacy paradox: An experimental look at advertising personalization, public policy and public understanding. Cyberpsychology: Journal of Psychosocial Research on Cyberspace 10 (1).

Burgoon, J. K. 1982. Privacy and Communication. Annals of the International Communication Association 6: 206-249.

Culnan, M.J. and Armstrong, P.K. 1999. Information privacy concerns procedural fairness and impersonal trust: an

empirical investigation. Organization Science 10 (1): 104–115.

De Keyzer, F., van Noort, G., and Kruikemeier, S. 2022. Going too far? How consumers respond to personalized advertising from different sources. Journal of Electronic Commerce Research 23 (3): 138-159.

Desimpelaere, L., Hudders, L., and Van de Sompel, D. 2021. Children's perceptions of fairness in a data disclosure context: The effect of a reward on the relationship between privacy literacy and disclosure behavior. Telematics and Informatics 61: 101602.

Dietrich, C. 2010. Decision Making: Factors that Influence Decision Making, Heuristics Used, and Decision Outcomes. Inquiries Journal 2: 3.

Dijkstra, A. 2008. The Psychology of Tailoring-Ingredients in Computer-Tailored Persuasion. Social and Personality Psychology Compass 2: 765-784.

Dijkstra, A. and Ballast, K. 2012. Personalization and perceived personal relevance in computer-tailored persuasion in smoking cessation. British Journal of Health Psychology 17 (1): 60-73.

Dinev, T. and Hart, P. 2006. Privacy concerns and levels of information exchange: An empirical investigation of intended e-services use. E-Service 4 (3): 25-60.

Dinev, T., Xu, H., Smith, J., and Hart, P. 2013. Information Privacy and Correlates: An Empirical Attempt to Bridge and Distinguish Privacy-Related Concepts. European Journal of Information Systems 22: 295-316.

Ducoffe, R.H. 1995. How Consumers Assess the Value of Advertising. Journal of Current Issues & Research in Advertising 17 (1): 1-18.

Eisend, M., and Tarrahi, F. 2022. Persuasion knowledge in the marketplace: A meta-analysis. Journal of Consumer Psychology 32 (1): 3-22.

Fabrigar, L.R., Wegener, D.T., MacCallum, R.C. and Strahan, E.J. 1999. Evaluating the use of exploratory factor analysis in psychological research. Psychological methods 4 (3): 272.

Fornell, C., and Larcker, D.F. 1981. Evaluating structural equation models with unobservable variables and measurement error. Journal of Marketing Research 18 (1): 39-50.

Frick, T. W., and Li, T. 2016. Personalization in social retargeting - A field experiment. 2016 International Conference on Information Systems, ICIS 2016.

Gironda, J.T., and Korgaonkar, P.K. 2018. iSpy? Tailored versus invasive ads and consumers' perceptions of personalized advertising. Electronic Commerce Research and Applications 29: 64-77.

Hair, J.F. Jr., Anderson, R.E., Tatham, R.L., and Black, W.C. 2006. Multivariate Data Analysis (6th ed.). New Jersey. Prentice-Hall.

Ham, C.D. 2017. Exploring how consumers cope with online behavioral advertising. International Journal of Advertising 36 (4): 632-658.

Hayes, A.F. 2017. Introduction to mediation, moderation, and conditional process analysis: A regression-based approach. Guilford Publications.

Hoffman, D., Novak, T., and Peralta, M. 1998. Information Privacy in the Marketspace: Implications for the Commercial Uses of Anonymity on the Web. The Information Society 15.

Hu, L.T., and Bentler, P.M. 1999. Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. Structural Equation Modeling: A Multidisciplinary Journal 6 (1): 1-55.

Karwatzki, S., Dytynko, O., and Veit, D. 2017. The Influence of Privacy Dispositions on Perceptions of Information Transparency and Personalization Preferences. Hawaii International Conference on System Sciences.

Kehr, F., Kowatsch, T., Wentzel, D., and Fleisch, E. 2015. Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. Information Systems Journal 25 (6): 607-635.

Kehr, F., Wentzel, D., and Mayer, P. 2013. Rethinking the privacy calculus: on the role of dispositional factors and affect.

Kline, P. 2015. A handbook of test construction (psychology revivals): introduction to psychometric design. Routledge.

Knijnenburg, B., Raybourn, E., Cherry, D., Wilkinson, D., Sivakumar, S., and Sloan, H. 2017. Death to the Privacy Calculus?

Kronemann, B., Kizgin, H., Rana, N., and K. Dwivedi, Y. 2023. How AI encourages consumers to share their secrets? The role of anthropomorphism, personalisation, and privacy concerns and avenues for future research. Spanish Journal of Marketing 27 (1): 3-19.

Kurtz, O.T., Wirtz, B.W., and Langer, P.F. 2021. An empirical analysis of location-based mobile advertising—Determinants, success factors, and moderating effects. Journal of Interactive Marketing 54 (1): 69-85

Lee, C.H., and Cranage, D.A. 2011. Personalisation-privacy paradox: the effects of personalisation and privacy

assurance on customer responses to travel web sites. Tourism Management 32: 987-994.

Lee, D.H., Im, S. and Taylor, C.R. 2008. Voluntary self-disclosure of information on the Internet: A multimethod study of the motivations and consequences of disclosing information on blogs. Psychology & Marketing 25 (7): 692-710.

Lee, D.J., Ahn, J.H. and Bang, Y. 2011. Managing consumer privacy concerns in personalization: a strategic analysis of privacy protection. Mis Quarterly 423-444.

Lee, J., Kim, S., and Ham, C.D. 2016. A double-edged sword? Predicting consumers' attitudes toward and sharing intention of native advertising on social media. American Behavioral Scientist 60 (12): 1425-1441.

Li, H., and Nill, A. 2020. Online Behavioral Targeting: Are Knowledgeable Consumers Willing to Sell Their Privacy? Journal of Consumer Policy 43: 723-745.

Li, P., Cho, H. and Goh, Z.H. 2019. Unpacking the process of privacy management and self-disclosure from the perspectives of regulatory focus and privacy calculus. Telematics and Informatics 41: 114-125.

Lin, C.A., and Kim, T. 2016. Predicting user response to sponsored advertising on social media via the technology acceptance model. Computers in Human Behavior 64: 710-718.

Lwin, M., and Williams, J. 2003. A Model Integrating the Multidimensional Developmental Theory of Privacy and Theory of Planned Behavior to Examine Fabrication of Information Online. Marketing Letters 14: 257-272.

Matic, A., Pielot, M., and Oliver, N. 2017. "OMG! How did it know that?": Reactions to Highly-Personalized Ads. Adjunct Publication of the 25th Conference on User Modeling, Adaptation and Personalization 41-46.

McKnight, D. H., and Chervany, N. L. 2002. What trust means in E-commerce customer relationships: An interdisciplinary conceptual typology. International Journal of Electronic Commerce 6 (2): 35–59.

Meyer, C., and Schwager, A. 2007. Understanding customer experience. Harvard Business Review 85 (2): 116.

Miltgen, C. L., Cases, A. S., and Russell, C. A. 2019. Consumers' responses to facebook advertising across PCs and mobile phones: A model for assessing the drivers of approach and avoidance of facebook ads. Journal of Advertising Research 59 (4): 414-432.

Miltgen, C.L., Cases, A.S., and Russell, C.A. 2019. Consumers' responses to facebook advertising across PCs and mobile phones: A model for assessing the drivers of approach and avoidance of facebook ads. Journal of Advertising Research 59 (4): 414-432.

Montgomery, K., Chester, J., Nixon, L., Levy, L. and Dorfman, L. 2019. Big Data and the transformation of food and beverage marketing: undermining efforts to reduce obesity?. Critical Public Health 29 (1): 110-117.

Morimoto, M. 2017. Information contents in Japanese OTC drug advertising from elaboration likelihood model perspective: content analysis of TV commercials and OTC drug websites. Journal of Promotion Management 23 (4): 575-591.

Morimoto, M. 2021. Privacy concerns about personalized advertising across multiple social media platforms in Japan: The relationship with information control and persuasion knowledge. International Journal of Advertising 40 (3): 431-451.

Mpinganjira, M., and Maduku, D.K. 2019. Ethics of mobile behavioral advertising: Antecedents and outcomes of perceived ethical value of advertised brands. Journal of Business Research 95: 464-478.

Okazaki, S., Li, H., and Hirose, M. 2009. Consumer privacy concerns and preference for degree of regulatory control. Journal of Advertising 38 (4): 63-77.

Paschal, J.L., Stone, D.L., and Stone-Romero, E.F. 2009. Effects of electronic mail policies on invasiveness and fairness. Journal of Managerial Psychology 24 (6): 502-525.

Phelps, J., D'Souza, G., and Nowak, G. 2001. Antecedents and consequences of consumer privacy concerns: An empirical investigation. Journal of Interactive Marketing 15 (4): 2-17.

Piao, C., Li, X., Pan, X., and Zhang, C. 2016. User privacy protection for a mobile commerce alliance. Electron. Commer. Res. Appl. 18: 58-70.

Sheehan, K.B. and Hoy, M.G. 1999. Flaming, complaining, abstaining: How online users respond to privacy concerns. Journal of Advertising 28 (3): 37-51.

Shevlin, M. and Miles, J.N. 1998. Effects of sample size, model specification and factor loadings on the GFI in confirmatory factor analysis. Personality and Individual Differences 25 (1): 85-90.

Srinivasan, S.S., Anderson, R., and Ponnavolu, K. 2002. Customer loyalty in e-commerce: an exploration of its antecedents and consequences. Journal of Retailing 78 (1): 41-50.

Steenkamp, J.B.E., and Baumgartner, H. 1998. Assessing measurement invariance in cross-national consumer research. Journal of Consumer Research 25 (1): 78-90.

Steiger, J.H. 2007. Understanding the limitations of global fit assessment in structural equation modeling. Personality and Individual Differences 42 (5): 893-898.

Sun, Y., Wang, N., and Shen, X.L. 2021. Calculus interdependency, personality contingency, and causal asymmetry: Toward a configurational privacy calculus model of information disclosure. Information & Management 58 (8): 103556.

Tabachnick, B.G., and Fidell, L.S. 2007. Experimental designs using ANOVA. Belmont, CA: Thomson/Brooks/Cole 74

Taddicken, M. 2014. The 'privacy paradox'in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. Journal of Computer-Mediated Communication 19 (2): 248-273.

Taj, S.A. 2016. Application of signaling theory in management research: Addressing major gaps in theory. European Management Journal 34 (4): 338-348.

Taylor, D.G., Lewin, J.E. and Strutton, D. 2011. Friends, fans, and followers: do ads work on social networks? how gender and age shape receptivity. Journal of Advertising Research 51(1): 258-275.

Tepper, B.J., and Braun, C.K. 1995. Does the experience of organizational justice mitigate the invasion of privacy engendered by random drug testing? An empirical investigation. Basic and Applied Social Psychology 16 (1-2): 211-225.

Thibodeaux, H.F., and Kudisch, J.D. 2003. The relationship between applicant reactions, the likelihood of complaints, and organization attractiveness. Journal of Business and Psychology 18: 247-257.

Tucker, C.E. 2014. Social networks, personalized advertising, and privacy controls. Journal of Marketing Research 51 (5): 546–56.

Urban, G., Amyx, C., and Lorenzon, A. 2009. Online Trust: State of the Art, New Frontiers, and Research Potential. Journal of Interactive Marketing 23: 179-190.

Van Doorn, J., and Hoekstra, J. C. 2013. Customization of online advertising: The role of intrusiveness. Marketing Letters 24: 339-351.

Venkatesh, V., Morris, M.G., Davis, G.B., and Davis, F.D. 2003. User acceptance of information technology: Toward a unified view MIS quarterly: 425-478.

Wang, L., Hu, H.H., Yan, J., and Mei, M.Q. 2020. Privacy calculus or heuristic cues? The dual process of privacy decision making on Chinese social media. Journal of Enterprise Information Management 33 (2): 353-380.

White, T. B., Zahay, D. L., Thorbjørnsen, H., and Shavitt, S. 2008. Getting too personal: Reactance to highly personalized email solicitations. Marketing Letters 19: 39-50.

Wieczorkowski, J., and Polak, P. 2017. Big data and privacy: The study of privacy invasion acceptance in the world of big data. Online Journal of Applied Knowledge Management 5: 57-71.

Wilson, D.W. and Valacich, J. 2012. Unpacking the Privacy Paradox: Irrational Decision-Making within the Privacy Calculus. International Conference on Information Systems, ICIS 2012 5: 4152-4162.

Xu, D.J. 2006. The influence of personalization in affecting consumer attitudes toward mobile advertising in China. Journal of Computer Information System 47(2): 9-19.

Xu, H., Dinev, T., Smith, H.J., and Hart, P. 2011. Information privacy concerns: linking individual perceptions with institutional privacy assurances. Journal of the Association for Information Systems 12 (12): 798–824.

Xu, Z., and Zhou, Y. 2013. Relevance Theory and Its Application to Advertising Interpretation. Theory and Practice in Language Studies 3 (3): 492-496.

Zhao, W., and Othman, M.N. 2011. Predicting and explaining complaint intention and behaviour of Malaysian consumers: an application of the planned behaviour theory. International Marketing 21: 229-252

Zhu, Y.Q., and Chang, J.H. 2016. The key role of relevance in personalized advertisement: Examining its impact on perceptions of privacy invasion, self-awareness, and continuous use intentions. Computers in Human Behavior 65: 442-447.