

Consumers perspective of online behavioral advertising (OBA): The integration of persuasion knowledge model (PKM) and protection motivation theory (PMT)

Ahmad Zulfahmi* and Adi Zakaria Affif

Master of Management Faculty of Economic and Business University of Indonesia, Jakarta, Indonesia

E-mail address: azulfahmi86@gmail.com

Abstract - This study examines how consumer knowledge about online behavioral advertising (OBA) tactics affects ad avoidance behavior in display ads and video ads on Instagram social media platforms. The study combines two theoretical approaches, the Persuasion Knowledge Model (PKM) and the Protection Motivation Theory (PMT). The online survey examined how consumers cope with OBA based on their persuasion knowledge, cognitive appraisal, and cognitive processing variables. Structural equation modeling was used to analyze the data collected from 211 consumers aged 18-34 years who are active Instagram users. The results reveal that from the cognitive appraisal variables, the perceived risks were indirectly associated with ad avoidance throughout privacy concerns without being related to persuasion knowledge, perceived benefits were significantly associated with persuasion knowledge. Still, it was not associated with privacy concerns, persuasion knowledge was indirectly associated with ad avoidance throughout self-efficacy, and privacy concerns partially mediated such associations with ad avoidance. From the cognitive processing variables, reactance was significantly associated with ad avoidance without being related to persuasion knowledge, and perceived personalization was associated with persuasion knowledge and significantly related to ad avoidance.

Keywords - Online behavioral advertising, Online privacy concerns, Ad avoidance, Persuasion knowledge, Protection motivation, Digital marketing, Instagram

I. INTRODUCTION

Based on the digital report from Hootsuite & We Are Social 2021, Indonesian internet users in January 2021 have reached 202.6 million people, or around 73.7% of Indonesia's current total population of 274.9 million people. With this number of users, this is a massive potential for marketers in Indonesia to market their product's digital marketing. However, in Indonesia, the use of the Internet is still dominated by social media as the main activity on the Internet. Out of 202.6 million internet users in Indonesia, 170 million are active users of social media. And if viewed from the average daily internet usage in Indonesia, the average daily internet usage time is 8 hours 52 minutes per day, 3 hours and 14 minutes were spent using social media [1].

Of the top five most used social media platforms in Indonesia, three of them are platforms from the Facebook network (Facebook, Whatsapp, and Instagram), which is

used by around 80% of the total population in Indonesia [1]. Seeing this development of internet use in Indonesia, it is essential to know consumers' perspectives on the benefits and risks of using the Internet, especially in digital marketing.

One of the most important new ways to reach targeted audiences in digital marketing is with Online Behavioral Advertising (OBA) [2]. The use of OBA allows companies to target consumers more accurately by studying the footprint of consumer data on the Internet, such as browsing or shopping history [3]. Boerman et al. state that online behavioral advertising is a practice of monitoring people's online behavior and using the collected information to show people individually targeted advertisements [4].

Citing research conducted by Baek and Morimoto [5], Data collected in OBA practice can include sensitive personal information such as health, finances, or children. This kind of sensitive information may fall into the hands of irresponsible parties or be used for unexpected purposes and increase consumer fears about losing control of their sensitive personal information [5]. Several studies have revealed a lack of consumer perceptions and knowledge of OBA practices and the associated privacy issues and regulations [6]–[8]. Not many consumers are aware of the practice of tracking online behavior, and know-how tailored advertising messages are delivered [6], [8].

One of the studies that discuss the impact of OBA is Research by Chang-Dae Ham [9]. This study examines the effects of knowledge about persuasion in OBA on privacy concerns and ad avoidance. Research conducted on college students using an ad format in the form of a display ad on websites and ad networks found that respondents were more likely to avoid OBA when they recognized a higher level of covert persuasion tactics; receive more of the potential risks and fewer benefits of OBA [9].

The research model developed by Chang-Dae Ham [9] uses the integration of two theories in building his research model, namely the Persuasion Knowledge Model [10] and Protection Motivation Theory [11]. First, this research uses the Persuasion Knowledge Model approach, which wants to see how the influence of consumer knowledge persuasion on cognitive appraisal consisting of threat appraisal (severity/reward) and coping appraisal (self-efficacy) and also on cognitive processing consisting of reactance and perceived personalization. Furthermore, the PKM model is integrated into the Protection Motivation Theory model, which wants to examine the effect of

knowledge persuasion on protection motivation (privacy concern), which wants to see whether ad avoidance will occur or not.

Considering that Chang-Dae Ham's [9] research has a solid theoretical foundation and has only been tested on respondents in the student group, this study seeks to test the model further using display and video ads formats in the Instagram social media platform. Moreover, in the broader group of respondents, namely students, employers, and workers in the 18-34 age range. Because this age range is the most extensive age range for social media users based on the Indonesia Digital Report 2021 report done by Hootsuite and We Are Social.

II. LITERATURE REVIEW

A. Online Behavioral Advertising (OBA)

For online marketers and advertisers, the current trend is to target more specific consumers because they understand that irrelevant advertising messages will only cause distraction, and consumers will avoid advertisements. Thus, efforts to convey more relevant advertising messages are critical in a digital world where there are many ad interruptions (for example pop-up ads and junk email) which significantly disrupt the consumer experience in using a website [5]. In such environmental conditions, Online Behavioral Advertising (OBA) provides the optimal solution for advertisers who do not want to waste money on advertising and reach people who have no interest in what they have to offer.

Online Behavioral Advertising (OBA) Is a technology in online advertising to deliver online advertisements that have been tailored to consumer interests and taste based on information that has been collected from consumer behavior on the Internet [2]. The main goal of OBA is to increase sales and profits by personalizing advertising content based on consumer characteristics [12]. Meanwhile, OBA is described as a technology-based advertising targeting method. Where digital media companies and advertising networks carry out tracking, collect online consumer behavior, conduct analysis, then infer interests, preferences, geographic location, etc. to then selectively expose tailored advertising messages to the same individual consumer [13].

The most common mechanism used in OBA is by using cookies from third parties. Third parties (for example, ad networks such as Facebook or Google) that work with specific websites visited by consumers can place cookie files on the consumer's hard drive without the consumer knowing it, thereby enabling the third party to identify consumer computer devices and track consumer online behavior for targeting purposes. Advertisements to these consumers.

With the application of OBA, consumers get more valuable and relevant advertising information without facing random and irrelevant advertisements [8], [14], [15]. However, in practice, OBA does online activity tracking,

collects behavioral data, and disseminates information that is often contrary to consumer privacy, especially given that very few webs or applications provide consumers with the option to consent to OBA's covert tracking tactics. Moreover, due to this covert mechanism, not many consumers understand how cookies from third parties are used in OBA practices and how their personal online activities are tracked.

This covert method can harm consumers when a consumer's online behavior is tracked without the consumer's knowledge or complete awareness of the potential risk of privacy breaches. Research has found that personalized advertising poses significant privacy concerns due to the potential to misuse personal information [5], [16], [17]. OBA will raise serious concerns, especially because consumers do not clearly understand how OBA works and how to control what information from the online behavior they can share.

B. Persuasion Knowledge Model (PKM) and Privacy Concern

OBA is a technology-driven persuasion tactic that is covert and difficult for consumers to deal with effectively because it is invisible [6], [18], [19]. To understand and interpret how consumers deal with these hidden tactics, in this study, Chang-Dae Ham [9] argue that the Persuasion Knowledge Model (PKM) approach is the proper framework. In their Research, Friestad and Wright [10] suggest that in responding to the persuasion efforts of persuasion agents (for example, marketers or advertisers), consumers as persuasion targets should be able to conclude what the hidden motives of a persuasion attempt (advertising) are.

When the main intentions of the persuasion tactic can be revealed, the consumer can actively overcome the persuasion effort. Furthermore, in this study, recognizing the hidden persuasion intentions of advertisers may activate a level of consumer knowledge of persuasion efforts, which in turn may lead consumers to resist persuasion by persuasion agents (advertisers or marketers). In the context of OBA, with the fact that OBA uses cookies as a covert marketing tactic [19], PKM can be interpreted as the extent to which consumers' knowledge and understanding of the use of cookies in OBA is a covert marketing tactic in dealing with an online advertisement.

Information privacy is defined as an individual's ability to control when, how, and the extent to which his personal information is communicated to others [20]. The increase in the digitization of personal information and advances in Internet technology poses new challenges for consumer information privacy [21]–[23]. On the one hand, personalized web services and business software require collecting and extracting large amounts of personally identifiable information [24]. So; on the other hand, when consumers become content providers on web blogs and social networking sites, their personal information becomes more vulnerable.

Concern which represents consumers' beliefs, attitudes, and perceptions about their privacy, has been used as a proxy measure in many contexts [25]. Treated as antecedent [26], [27], as consequence [28], [29], as mediator [30], [31], and as a moderating factor [21], [32]. According to [33] attention to privacy varies depending on attitudes towards marketers, situational characteristics, and shopping habits which ultimately affect consumers' willingness to provide data to marketers.

Concerning PKM, when consumers are not aware of the practice of collecting and tracking their personal information data, there will be a risk of misuse of that personal information as a result of consumers being unable to control what personal information data they can share.

Research on consumer persuasion knowledge has been expanded into the context of consumer privacy concerns about personalized advertising and disclosure of personal information on a website, but the results have not been consistent. Simonson [34] found that consumers acknowledge tailored claims of personalized advertising messages as an attempt at manipulative persuasion. Youn [35] examined the relationship between the general knowledge of young people about personal information practices on websites and the privacy issues arising from such practices but did not find a significant relationship between them. Neither of these studies has directly examined the relationship between knowledge of persuasion and privacy concerns.

However, it is implied that consumer persuasion knowledge is related to the level of concern about privacy violations in personalized advertising. Given the fact that OBA using third-party cookies as a covert marketing tactic [19] and assumes a positive relationship between persuasion knowledge and issues of privacy violations. Chang-Dae Ham [9] states that consumer knowledge of persuasion techniques (persuasion knowledge), which arises from the acknowledgment that OBA uses covert third-party cookies, will have a positive relationship with consumer concerns about privacy (privacy concern) on OBA. So that the hypothesis that is formed is as follows:

H1: Consumer persuasion knowledge about OBA has a positive effect on privacy concern on OBA

C. Persuasion Knowledge Model and Coping Strategies

According to the PKM theory, consumers with better persuasion knowledge are more likely to develop effective coping strategies for persuasion techniques [35], [36]. Effective coping strategies against persuasion techniques, as described by Kirmani and Campbell [37], are not necessarily a stronger resistance to persuasion techniques but rather a better understanding and assessment of the effectiveness of a persuasion technique. Consumers as the target of OBA who have better persuasion knowledge about OBA will be better able to understand what the effects of OBA persuasion are; they will therefore pursue potential benefits or avoid possible harm from OBA and will thus consider that they have achieved personal goals

as a result of their interactions with OBA [9]. Therefore, the hypothesis formed is as follows:

H2a: Consumer persuasion knowledge of OBA has a positive effect on the perceived risk of OBA

H2b: Consumer persuasion knowledge of OBA has a positive effect on the perceived benefits of OBA

D. Protection Motivation Theory (PMT) and Cognitive Appraisal

Protection Motivation Theory (PMT) tries to explain how individuals perceive threats in an environment with risks and copes with them based on cognitive assessments. This theory introduces six factors into two cognitive mechanisms: the threat appraisal mechanism consisting of perceived severity, perceived vulnerability, and reward and coping appraisal mechanisms consisting of perceived response efficacy, perceived self-efficacy, and response cost. These assessment processes are involved in the motivation to protect oneself and perform adaptive behavior in response to risky events [9]. Several previous studies explained that PMT provides a basic framework to explain how people behave in response to certain types of threats or fears in various contexts such as smartphone security [38], health risks [39], and privacy on social media [40].

In the threat appraisal process for PMT, the perception of the threat level is determined by the difference between the combined severity of risk and vulnerability, on the one hand, with reward, on the other hand. (Threat appraisal = severity and vulnerability of risk - reward) [9].

In the threat assessment process of PMT, this theory proposes that individual assessments of risks and benefits play an essential role in activating consumer protection motivation. Thus, any perceived loss (risk) associated with risky behavior will increase consumer protection motivation, while on the contrary, any perceived reward (benefit) will reduce consumer protection [11], [41], [42].

In the context of OBA, vulnerability to risk refers to the perception of the possibility that losses will occur to the privacy of individual consumers as a result of disclosing information through OBA. The severity of risk refers to the perception of how much harm may arise to consumer privacy due to disclosing information through OBA [9].

According to PMT [11], vulnerability and severity are different assessment processes but combined to form effective coping strategies by individuals. With this framework and applying the expectancy-value approach ($\sum s_i v_i$; s: severity, v: vulnerability), risk perception is calculated as a combination of vulnerability and severity that together significantly influences risk management strategies [43]. Thus, the hypothesis formed is as follows:

H3a: Perceived vulnerability to a severe risk of privacy breaches (perceived risk) will positively affect concerns about consumer privacy issues on OBA (privacy concern).

Benefits in PMT refer to the rewards that consumers expect by engaging in risky behavior. When the benefits of obtaining relevant information from OBA outweigh the risks received from a breach of privacy, it reduces the motivation to protect privacy [33], [44]. White [45] reveals that consumers are willing to share personal information related to privacy in exchange for customized marketing offers. In addition, users of social networking sites are willing to disclose their information to maintain social relationships with their friends [46] and to meet their needs [47]. In these study, an increase in perceived benefits will reduce defensive motives. Chang-Dae Ham [9] states that consumers are less likely to worry about privacy violations when they feel more benefits from OBA, which provides relevant information to consumers. Therefore the hypothesis that is formed is:

H3b: Perception of the benefits (perceived benefits) of receiving relevant information has a negative effect on the concern of privacy concerns on OBA.

Apart from threat appraisal, PMT also proposes another cognitive mechanism in coping appraisal, in which there are three significant factors in influencing protection motivation: perceived self-efficacy, perceived response efficacy, and response costs. Among these variables, self-efficacy refers to the level of individual confidence in their ability to achieve specific goals [48]. In the context of online privacy, the concept of self-efficacy refers to an individual's confidence in their ability to protect online privacy [49], [50].

Previous studies have consistently shown that the concept of self-efficacy is a significant predictor of concern about privacy infringement. Individuals with higher levels of self-efficacy tend to have lower attention to the privacy of health information [51], self-efficacy significantly affects privacy issues in social networks [52] and engage in social behavior protection against viruses [53].

According to Bearden et al. [54], persuasion knowledge is a sub-dimension of the concept of self-confidence, representing the perception of consumers' ability to understand persuasion agent tactics and their ability to overcome these tactics. Therefore, consumer knowledge persuasion is conceptually associated with self-efficacy so that those who have higher knowledge persuasion will have higher self-efficacy in responding to persuasion tactics that pose a threat [9]. In his research, Chang-Dae Ham [9] states that consumer persuasion knowledge is positively related to self-efficacy, which will be a significant factor predicting consumer judgment about how to deal with possible privacy violations by OBA. Thus, the hypothesis is:

H4a: Consumer persuasion knowledge of OBA has a positive effect on self-efficacy

H4b: Self-efficacy has a positive effect on privacy concern with OBA

E. Advertising Avoidance as Coping Behavior

The Internet is a task-and-goal-oriented medium whereby users quickly avoid advertisements when they are perceived to interfere with achieving their goals [55]–[57]. Ad avoidance refers to all actions by media users that differently reduce their exposure to advertising content [58].

In the context of the Internet, Cho and Cheon [56] explain that advertising avoidance includes three components in terms of consumer response to advertisements on the Internet, namely: cognitive, affective, and behavioral. Applying this theory to the context of OBA, cognitive avoidance of advertising will involve willfully ignoring advertising messages conveyed through behavioral targeting. Affective avoidance of advertising will occur when consumers dislike or hate advertising messages that have been tailored by tracking behavior. Behavioral ad avoidance represented by consumer action to avoid the ad by immediately leaving the OBA page, blocking the OBA, or avoiding clicking on the OBA [9].

Consumer protection motivation arising from OBA-related privacy concerns will positively influence their protective behavior in the form of advertising avoidance [9]. Therefore the hypothesis that is formed is:

H5: Privacy concern of consumers regarding OBA will have a positive effect on ad avoidance

F. Persuasion Knowledge Model Effect on Psychological Reactance and Perceived Personalization

Psychological reactance theory [59] suggests that any attempt that aims to change or control a person's attitude or behavior can be considered a threat to individuals as well as a threat to their freedom. When their freedom is limited, threatened, or lost, consumers will try to restore it. This motivation for recovery is known as psychological reactance, encouraging consumers to react the opposite way to persuasion attempts [60], [61]. Meanwhile, according to Steindl et al. [62] psychological reactance is a reaction to the threat to freedom that arises from a persuasive message. Where it is defined as an unpleasant motivational that arises when a person experiences a threat or potential loss of freedom [62].

Psychological reactance mediates the personalization effect because it limits personal freedom to manage and control personal information and privacy [63]. Persuasion knowledge behavior tracking methods in OBA can be seen as limiting personal freedom to control and protect personal privacy online, which in turn increases psychological reactance. Furthermore, it is hoped that the psychological reactance will motivate consumers to react negatively and increase OBA avoidance rather than accepting it [9]. The hypothesis that is formed is as follows:

H6a: Consumer persuasion knowledge of OBA has a positive effect on reactance

H6b: Reactance has a positive effect on ad avoidance

Personalization can be defined as the delivery of personalized advertisements to individuals based on their exclusive preferences [64]. Persuasion knowledge allows consumers to see the effectiveness of a persuasion tactic [10]. In theory, perceived effectiveness refers to the perception of “what makes a persuasion tactic effective [37]. In the context of OBA, Chang-Dae Ham [9] argues that perceived effectiveness means the extent to which consumers perceive that OBA messages have been personalized for them, or what is called perceived personalization.

When consumers know and understand how OBA works, they will tend to see OBA personalization; thus, persuasion knowledge will be positively related to perceived personalization [9]. Perceived personalization is negatively related to ad avoidance because the more personalized it is, the more valuable the advertisement is, and the less likely it is to cause ad avoidance [5]. Therefore, persuasion knowledge about OBA will be positively related to perceived personalization, which in turn will be negatively related to OBA avoidance [9]. The hypothesis that is formed is as follows:

H7a: Consumer persuasion knowledge of OBA has a positive effect on perceived personalization

H7b: Perceived personalization has a positive effect on ad avoidance

G. Reactance and Perceived Personalization on Protection Motivation Theory

In PMT theory, reactance and perceived personalization variables are not conceptualized as assessment variables related to motivation in privacy protection, but in Chang-Dae Ham's [9], these two variables are tried to examine how the relationship between these two variables is on privacy concern. According to Chang-Dae Ham [9], it is said that reactance is the opposite reaction of consumers to the purpose behind persuasion tactics; therefore, reactance may be related to the motivation of privacy protection. In addition, perceived personalization may be positively related to privacy concern wherein perceived personalization will increase privacy concern or be negatively related to privacy concern to the extent that perceived personalization would increase perceived usefulness, decreasing motivation to protect privacy.

From Chang-Dae Ham's [9] on the relationship between the two variables reactance and perceived personalization to privacy concern, it was found that reactance has a positive and significant relationship to privacy concern while perceived personalization has a positive relationship

to privacy concern but not significant. Regarding the explanation above, this study will also examine the relationship between reactance to privacy concerns and also the relationship between perceived personalization to privacy concerns and the hypothesis formed as follows:

H8a: Reactance has a positive effect on privacy concerns

H8b: Perceived personalization has a positive effect on privacy concern

H. Reactance and Perceived Personalization on Protection Motivation Theory

In previous studies such as Crossler [65] and Chang-Dae Ham [9], cognitive appraisal variables, namely perceived risk, perceived benefit, and self-efficacy, can be directly related to protective behavior as in theory PMT. Chang-Dae Ham [9] shows that perceived risk and self-efficacy positively and significantly affect ad avoidance behavior, while perceived benefit has a negative but not significant effect on ad avoidance behavior. By referring to the results of the previous research, this study will also examine the relationship of the three cognitive appraisal variables to ad avoidance behavior with the hypothesis formed, namely:

H9a: Perceived risk has a positive effect on ad avoidance behavior

H9b: Perceived benefit has a negative effect on ad avoidance behavior

H9c: Self-efficacy has a positive effect on ad avoidance behavior

By integrating two-approach models, Persuasion Knowledge Model [10] and Protection Motivation Theory [11], this study applied the conceptual model from Chang-Dae Ham [9] is as follows:

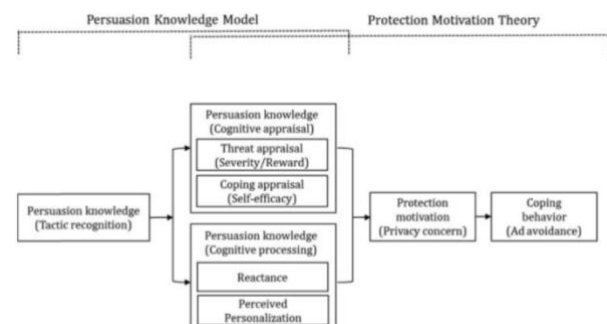


Fig. 1. Chang-Dae Ham (2017) conceptual model.

II. METHODOLOGY

A. Participants and Procedure

A total of 373 respondents has participated in a survey that was shared through a google form. Participants read the definition of OBA and then answered questions to screen for conditions: whether they had experienced OBA in Instagram during the last six months. Given that most consumers do not correctly understand how OBA works, OBA's definition and examples were presented to avoid any unnecessary misunderstanding that might mistakenly lead respondents to give answers about other types of advertising [9].

The other three screening questions were about their age, how many times a day they use social media, and whether they have an Instagram account. Referring to the Indonesian digital data from Hootsuite & We Are Social 2021, most social media users are between 18-34 years old and use social media 3 hours a day on average. So we are focusing on this scope to make this research more relevant, and because this research aims to see the perception of consumers about OBA in Instagram, so it is essential to make sure that the participants are Instagram users.

After the screening process, participants answered a series of questions about OBA in the primary survey. Among all 373 original participants, a total of 211 (56.5%) satisfied the four conditions: they had experience OBA in Instagram during the last six months, age between 18-34 years old, using social media 3 hours a day or more, and they have an Instagram account.

From final the respondents ranged between 18 to 34 years, Female participants 113 (53.6 %) outnumbered male 98 (46.4%), Respondents aged 18-22 years old were 79 people (37.44%), aged 23-27 years old were 68 people (32.23%) and aged 28-34 years old were 64 people (30.33%). The profession of the respondents are as follows: Private/state-owned company employees were 83 people (39.34%), Students were 88 people (41.71%), Entrepreneurs / Professionals were 16 people (7.58%), Civil Servants were 7 people (3.32 %), and others were 17 people (8.06%). Moreover, of the 211 respondents, as many as 116 people (54.98%) used social media for 3-5 hours a day, and the remaining 95 (45.02%) people used social media more than 5 hours a day.

B. Measurement

This research was conducted using a survey questionnaire instrument. The items of each construct were measured using a 6-point Likert scale, with 1 indicating strongly disagree and 6 expressing strongly agree. First, persuasion knowledge was measured by six items modified from those suggested by Bearden et al. (2001). Second, privacy concerns were measured on a six-item scale based on Dolnicar & Jordaan [66]. Third, ad avoidance was measured on a five-item scale based on the work of Baek & Morimoto [5], Cho & Cheon [56], and Elliott & Speck [58]. Fourth, self-efficacy was measured on a four-item

scale modified from Woon et al. [67], Crossler [65], and Larose & Rifon [68].

Fifth, the perceived risk was computed by multiplying perceived risk severity with the corresponding perceived risk vulnerability, and the resulting products were added to determine each risk factor $(\sum_{i=1}^n (severity)^i (vulnerability)^i)$ [9]. Sixth, to calculate the perceived benefit, each reward item was multiplied by its beneficiality as corresponding evaluation, and the results were added to arrive at each outcome factor $(\sum_{i=1}^n (reward\ belief)^i (beneficiality)^i)$ [9]. Next, reactance was measured by seven items modified from White et al. [69] and Hong & Faedda [70]. Finally, perceived personalization was measured by five items adapted from Dolnicar & Jordaan [66].

III. RESULTS

The model was tested using Lisrel 8.8 in a two-step process. First, a confirmatory factor analysis (CFA) was conducted to confirm the reliability and validity of the measurement model overall and each construct individually. The second step was to apply structural equation modeling (SEM) to examine the hypotheses in our proposed model.

A. Measurement Model

This section will discuss the results of testing the validity and reliability of all respondent data. The test results are in the table below:

TABLE I
RESULTS OF LOADING FACTOR AND T-VALUE

Variable	Indicator	loading factor	t-value	Validity
Persuasion Knowledge	PK1	0.83	14.45	Valid
	PK2	0.82	14.12	Valid
	PK3	0.83	14.45	Valid
	PK4	0.79	13.41	Valid
	PK5	0.66	10.38	Valid
	PK6	0.49	7.26	Valid
Perceived Risk	PR1	0.85	15.24	Valid
	PR2	0.88	16.09	Valid
	PR3	0.89	16.28	Valid
	PR4	0.89	16.38	Valid
Perceived Benefit	PB1	0.77	12.91	Valid
	PB2	0.80	13.58	Valid
	PB3	0.80	13.61	Valid
	PB4	0.86	15.20	Valid
	PB5	0.86	15.44	Valid
Self Efficacy	SE1	0.61	9.53	Valid
	SE2	0.87	15.62	Valid
	SE3	0.88	15.78	Valid
	SE4	0.87	15.55	Valid
Reactance	RA1	0.62	9.70	Valid
	RA2	0.38	5.51	Valid
	RA3	0.69	11.02	Valid
	RA4	0.84	14.67	Valid
	RA5	0.84	14.76	Valid
	RA6	0.85	14.87	Valid
	RA7	0.71	11.52	Valid
Perceived Personalization	PP1	0.85	14.93	Valid
	PP2	0.79	13.26	Valid
	PP3	0.79	13.43	Valid
	PP4	0.89	16.03	Valid
Privacy Concern	PC1	0.82	14.28	Valid
	PC2	0.85	15.00	Valid
	PC3	0.78	13.12	Valid
	PC4	0.91	16.73	Valid
	PC5	0.67	10.67	Valid
	PC6	0.70	11.45	Valid
Ad Avoidance	AA1	0.65	10.08	Valid
	AA2	0.82	13.89	Valid
	AA3	0.70	11.06	Valid
	AA4	0.56	8.34	Valid
	AA5	0.75	12.17	Valid

The validity test can be seen that the results are based on the loading factor value ≥ 0.5 and the t-value ≥ 1.65 (one-tailed) in table 1. All indicator items have a loading factor value of ≥ 0.5 except for the RA2 item in the reactance variable, but when viewed from the t-value, the RA2 item is still significant with a value of 5.51. The researcher concludes that the RA2 item in the reactance variable is still considered valid.

The reliability test is seen from the value of construct reliability (CR), where the cut-off is ≥ 0.7 and the AVE value ≥ 0.5 [71]. Table 2 shows that all variables in the model, both the CR value and the AVE value, are still above the cut-off value; thus, it can be concluded that the measurement scale is reliable.

TABLE II
RELIABILITY TEST RESULTS

Variable	Indikator	SLF	SLF ²	Measurement Error	CR	AVE	Reliability
Persuasion Knowledge	PK1	0,83	0,69	0,30	0,92	0,56	Reliabel
	PK2	0,82	0,67	0,32			
	PK3	0,83	0,69	0,30			
	PK4	0,79	0,62	0,37			
	PK5	0,66	0,44	0,56			
	PK6	0,49	0,24	0,76			
	Σ	4,42	3,35	1,69			
	Σ^2	19,54					
Perceived Risk	PR1	0,85	0,72	0,27	0,93	0,77	Reliabel
	PR2	0,88	0,77	0,22			
	PR3	0,89	0,79	0,21			
	PR4	0,89	0,79	0,20			
	Σ	3,51	3,08	0,90			
	Σ^2	12,32					
Perceived Benefit	PB1	0,77	0,59	0,41	0,91	0,67	Reliabel
	PB2	0,80	0,64	0,37			
	PB3	0,80	0,64	0,36			
	PB4	0,86	0,74	0,27			
	PB5	0,86	0,74	0,25			
	Σ	4,09	3,35	1,66			
	Σ^2	16,73					
Self Efficacy	SE1	0,61	0,37	0,62	0,89	0,67	Reliabel
	SE2	0,87	0,76	0,23			
	SE3	0,88	0,77	0,22			
	SE4	0,87	0,76	0,24			
	Σ	3,23	2,66	1,31			
	Σ^2	10,43					
Reactance	RA1	0,62	0,61	0,61	0,88	0,48	Reliabel
	RA2	0,38	0,85	0,85			
	RA3	0,69	0,53	0,53			
	RA4	0,84	0,30	0,30			
	RA5	0,84	0,29	0,29			
	RA6	0,85	0,28	0,28			
	RA7	0,71	0,50	0,50			
	Σ	4,93	3,36	3,36			
	Σ^2	24,30					
Perceived Personalization	PP1	0,85	0,72	0,28	0,90	0,69	Reliabel
	PP2	0,79	0,62	0,38			
	PP3	0,79	0,62	0,37			
	PP4	0,89	0,79	0,21			
	Σ	3,32	2,76	1,24			
	Σ^2	11,02					
Privacy Concern	PC1	0,82	0,67	0,33	0,91	0,63	Reliabel
	PC2	0,85	0,72	0,28			
	PC3	0,78	0,61	0,40			
	PC4	0,91	0,83	0,18			
	PC5	0,67	0,45	0,55			
	PC6	0,70	0,49	0,50			
	Σ	4,73	3,77	2,24			
	Σ^2	22,37					
Ad Avoidance	AA1	0,65	0,42	0,58	0,83	0,49	Reliabel
	AA2	0,82	0,67	0,33			
	AA3	0,70	0,49	0,51			
	AA4	0,56	0,31	0,69			
	AA5	0,75	0,56	0,44			
	Σ	3,48	2,46	2,55			
	Σ^2	12,11					

Before entering into hypothesis testing, the step necessary is to test the model fit. A model fit test needs to be done to evaluate whether this research model is suitable in describing every relationship between variables in the study. There are three categories of indexes that are commonly used to measure the fit of a research model:

1. Absolut Fit Indices which includes parameters such as GFI, RMSEA, and SMSR
2. Incremental Fit Indices which among them are NFI, NNFI, RFI, IFI, and CFI
3. Parsimony Fit Indices among which are PNFI, PGFI, and AGFI

From table 3 the results of the model fit test, it can be seen that this model is fit on the parameters belonging to the incremental fit indices category such as NFI with a value of 0.88 (marginal fit), NNFI with a value of 0.92 (good fit), CFI with a value of 0.92 (good fit), IFI with a value of 0.92 (good fit) and RFI with a value of 0.87 (marginal fit).

TABLE III
MODEL FIT TEST RESULTS

Category	Goodness of Fit Indices	Cut-off Value	Model Estimation Result
Absolute Fit Indices	Goodness of Fit Index (GFI)	≥ 0.90	0.67
	Root Mean Square Error of Approximation (RMSEA)	< 0.08	0.092
	Standardized Root Mean Residual (SRMR)	< 0.09	0.17
Incremental Fit Indices	Normed Fit Index (NFI)	≥ 0.90	0.88
	Non Normed Fit Index (NNFI)	≥ 0.90	0.92
	Comparative Fit Index (CFI)	≥ 0.90	0.92
	Incremental Fit Index (IFI)	≥ 0.90	0.92
	Relative Fit Index (RFI)	≥ 0.90	0.87
Parsimony Fit Indices	Parsimony Normed Fit Index (PNFI)	≥ 0.90	0.82
	Parsimony Goodness of Fit Index (PGFI)	≥ 0.90	0.60
	Adjusted Goodness of Fit Index (AGFI)	≥ 0.90	0.63

B. Hypothesis Testing

Hypothesis testing is done by using the Maximum Likelihood (ML) method. In addition, testing the relationship between the dependent and independent variables was carried out by looking at the significance based on the comparison between the t-statistic value generated by Lisrel and the t-table based on one tailed 5% alpha level (1.645). The test results for each hypothesis are explained as follows:

The relationship between persuasion knowledge and privacy concern has a positive coefficient of 0.04, but when viewed from the t-statistic value, the effect of persuasion knowledge on privacy concern is 0.57 where this value is lower than the t-table with 5% alpha, which is 1.645. Thus, it means that the hypothesis is rejected, and it is stated that the effect of persuasion knowledge on privacy concerns is not significant.

The effect of persuasion knowledge and perceived risk has a positive coefficient value of 0.09, but the t-statistic value test results show that persuasion knowledge has no significant effect on the perceived risk because it only has a t-value of 1.20, where this value is smaller than the t-table is 1.645; thus hypothesis 2a is rejected. On the other hand, the effect of persuasion knowledge on perceived benefits has a positive coefficient of 0.43 with a t-statistic value of 5.63, which means that knowledge persuasion has a positive and significant effect on perceived benefits; thus, hypothesis 2.b is accepted.

It was found that perceived risk had a positive and significant effect on privacy concern with a coefficient value of 0.68 with a t-statistic value of 9.66, and thus hypothesis 3.a was accepted. This further shows that

consumer's perceptions of risk will affect awareness of privacy issues in the context of OBA. The test results show that perceived benefits and privacy concern have a positive relationship with a coefficient of 0.003. The t-statistic significance level is 0.04; thus, the effect of perceived benefits on privacy concern is not significant, and hypothesis 3.b is rejected.

There is a positive and significant effect between persuasion knowledge and self-efficacy with a coefficient value of 0.37 and a t-statistic of 4.63; thus, hypothesis 4.a is accepted. There is a negative effect between self-efficacy and privacy concern with a coefficient value of -0.2, which means that the higher the level of consumer confidence in their ability to avoid OBA, the more consumers will see that privacy issues are not a serious problem. From this test, the t-statistic significance level between self-efficacy and privacy concern is -3.12, where this shows a significant effect. This result is different from the hypothesis, which proposes a positive and significant effect between self-efficacy and privacy concern, so hypothesis 4.b is rejected.

From the tests conducted, there is a positive effect between privacy concern and ad avoidance with a coefficient value of 0.32 and a t-statistic value of 3.42; thus, it is stated that there is a significant positive effect between privacy concern and ad avoidance, and hypothesis 5 is accepted. This means that the more a consumer is aware of the privacy risks of OBA, the more it will make them try to avoid OBA advertisements.

There is an effect between persuasion knowledge and reactance with a coefficient value of -0.01 and a t-statistic value of -0.07; thus, it is stated that there is no significant positive effect between persuasion knowledge and reactance, and hypothesis 6.a is rejected. From the tests conducted, there is a positive effect between reactance and ad avoidance with a coefficient value of 0.64 and a t-statistic value of 6.19; thus, it is stated that there is a significant positive effect between reactance and ad avoidance, and hypothesis 6.b is accepted.

From the tests conducted, it can be seen that there is an effect between persuasion knowledge on perceived personalization with a coefficient value of 0.34 and a t-statistic value of 4.51; thus, it is stated that between persuasion knowledge and perceived personalization, there is a significant positive effect and hypothesis 7.a is accepted. There is a negative effect between perceived personalization on ad avoidance with a coefficient value of -0.10. This is in line with the theory that when consumers feel that OBA ads have been adjusted to their needs, they will not avoid OBA advertisements. And from the t-statistic value, which is -1.71, this negative effect is declared significant, and thus hypothesis 7.b is accepted.

There is a positive effect between reactance and privacy concern with a coefficient value of 0.18 and a t-statistic value of 3.01, this positive effect is declared significant, and thus hypothesis 8.a is accepted. There is a positive effect between perceived personalization and privacy concern with a coefficient value of 0.06. However, from the t-statistic value, which is only 1.06, this positive effect

is declared insignificant, and thus hypothesis 8.b is rejected.

From the result of the test, there is a positive effect between perceived risk on ad avoidance with a coefficient value of 0.15, and this is in line with the theory that when a consumer feels that OBA advertisements have risk, they will avoid OBA advertisements. From the t-statistic value, which is 1.77, this positive effect is declared significant, and thus hypothesis 9.a is accepted. There is a negative effect between perceived benefit on ad avoidance with a coefficient value of -0.05. However, from the t-statistic value, which is only -0.89, this negative effect is declared insignificant, and thus hypothesis 9.b is rejected. And finally, there is a positive effect between perceived risk on ad avoidance with a coefficient value of 0.22, with a t-statistic value of 3.33, this positive effect is declared significant, and thus hypothesis 9.c is accepted.

TABLE IV
HYPOTHESIS TEST RESULT

Hypothesis	Path	Coefficients	t-value
H1	PK -> PC	0.04	0.57
H2a	PK -> PR	0.09	1.20
H2b	PK -> PB	0.43	5.63
H3a	PR -> PC	0.68	9.66
H3b	PB -> PC	0.003	0.04
H4a	PK -> SE	0.37	4.63
H4b	SE -> PC	-0.20	-3.12
H5	PC -> AA	0.32	3.42
H6a	PK -> RA	-0.01	-0.07
H6b	RA -> AA	0.64	6.19
H7a	PK -> PP	0.34	4.51
H7b	PP -> AA	-0.10	-1.71
H8a	RA -> PC	0.18	3.01
H8b	PP -> PC	0.06	1.06
H9a	PR -> AA	0.15	1.77
H9b	PB -> AA	-0.05	-0.89
H9c	SE -> AA	0.22	3.33

In this study, we also conducted a mediation test to see the role of privacy concern as a link in integrating the PKM-PMT model as proposed by Chang-Dae Ham [9], where privacy concern plays an important role in a driving factor for protective behavior in this case namely ad avoidance. From the results of the tests conducted, privacy concern does not have an indirect effect on the relationship between persuasion knowledge – ad avoidance (coefficient 0.03 and t-statistic 0.46), perceived benefit – ad avoidance (coefficient 0.04 and t-statistic 0.35), perceived personalization – ad avoidance (coefficient 0.04 and t-statistic 0.35), perceived personalization – ad avoidance (coefficient 0.06 and t-statistic 0.68).

Privacy concern has a positive and significant indirect effect on the relationship between reactance – ad avoidance (coefficient 0.16 and t-statistic 2.31). Privacy concern has a negative and significant indirect effect on the relationship between self-efficacy and ad avoidance (coefficient -0.20

and t-statistics - 3.06). Because the direct relationship between self-efficacy and reactance to ad avoidance also has a significant relationship, it can be concluded that privacy concern mediates the relationship between self-efficacy - ad avoidance and reactance - ad avoidance.

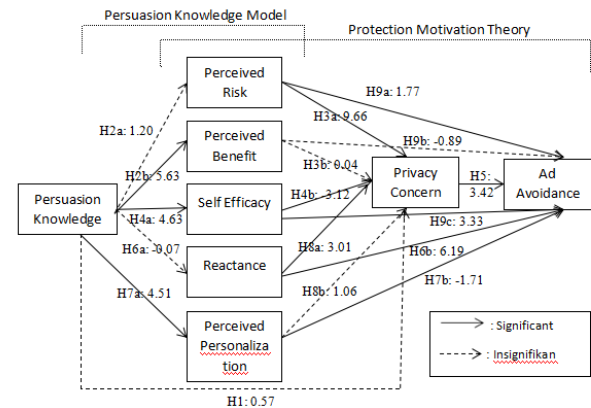


Fig. 1. Hypothesis final model.

IV. DISCUSSION

This research aims to explore how consumers cope with the persuasion tactics of OBA in social media Instagram. OBA is an interesting advertising practice providing both benefits (relevant messages) and risks (privacy infringements) to consumers; thus, consumers have ambivalent and paradoxical attitudes toward it [8]. The research conducted by Chang-Dae Ham [9] explains the trade-offs (risks and benefits) contained in OBA and how consumer strategy to cope with them. The integrated model proposed by Chang-Dae Ham [9] contributes to addressing unique aspects of consumer coping strategies: how consumers recognize the threat of persuasion tactics (persuasion knowledge); how such threat recognition is associated with threat appraisal (risk-benefit), coping appraisal (self-efficacy), and affective response processing (reactance; perceived personalization); and how these processes motivate protection behavior (privacy concerns; ad avoidance).

This study wanted to replicate the model from Chang-Dae Ham [9] and apply those research models to test how consumer coping strategies deal with persuasion techniques from OBA on social media Instagram. Given the difference in platforms, wherein Chang Dae Ham's research only tests within the scope of the website platform, we want to explore further how the proposed model explains the coping strategies of consumers on social media platforms, especially Instagram.

We found that persuasion knowledge was positively associated with perceived benefits and but not related to perceived risks. A positive association between persuasion knowledge and perceived benefits is in accordance with Chang-Dae Ham's [9] findings, which also refer to Kirmani & Campbel [37], where persuasion knowledge is an antecedent factor in assessing OBA benefits. However,

the persuasion knowledge is not related to the perceived risk in our findings, and This result is different from Chang-Dae Ham's [9] findings where it indicates that the perception of risk in OBA on social media Instagram is more determined by other factors outside of persuasion knowledge. Further research is needed to find out other factors that are the primary considerations of consumers on Instagram in assessing the risk of OBA.

Our next finding that perceived risk was positively associated with privacy concerns, whereas perceived benefit was not associated with privacy concerns, and privacy concern was positively related to consumer tendency to avoid OBA. This result is slightly different from Chang-Dae Ham [9] and some previous studies (e.g., [72]–[74]) suggesting that the risk and benefit assessment determines consumer attitudes intention of use and also in developing effective coping strategies. With these findings, we argue that consumers in social media Instagram only assess the perceived risk as the driving factor in developing coping strategies.

Our results reveal that perceived risk is a major factor in assessing privacy concerns without considering the benefits of receiving relevant messages from OBA. This is in line with the suggestion from Chang-Dae Ham [9] that perceived risk-benefit assessment depends on the context, and that perceived risk is greater in the OBA context because of its use of covert tactics and the lack of consumer knowledge about it. Interestingly, we found that self-efficacy has a significant negative association with privacy concerns. Contrary to the PMT suggests, we found that higher self-efficacy lowered privacy concerns, where these findings indicate that the higher the self-efficacy of consumers, the more they feel that privacy issues are not a cause for concern because they feel they will easily overcome them.

This study also tested cognitive appraisal variables (reactance and perceived personalization) to see the relationship between persuasion knowledge and protection motivation. We found that perceived personalization was significantly associated with persuasion knowledge, but reactance is not related to persuasion knowledge. In protection motivation, we found that reactance is directly positive related to ad avoidance, and perceived personalization is negatively related with ad avoidance.

This result implies that the more consumers consider the persuasion technique (cookies tracking) used by OBA is solely to provide personalized messages, the more consumers reduced their ad avoidance behavior. On the other hand, this finding also implies it is not persuasion knowledge that influences reactance in terms of ad avoidance, but it is the belief that the advertisement is intrusive that the end forms a psychological reactance to act against and avoid the advertisement. This finding is supported by the study from Chung & Kim [75], which found that perceived intrusiveness will encourage consumers to do ad avoidance, although further research must be carried out to see the relationship between reactance and perceived intrusiveness.

We also find that privacy concerns mediate the

relationship between reactance and ad avoidance and that the relationship between self-efficacy and ad avoidance differs from [9]. These results indicate that consumers on Instagram social media will still tend to avoid OBA ads without considering the risk and benefit assessment. This indicates that they feel that OBA ads interfere with the experience of using Instagram, so there must be a tendency to avoid, and privacy concerns are one of the factors driving the avoidance of these ads. This result is in line with the findings in the research of Lin & Kim [76], which found that intrusiveness concern and privacy concern are antecedent variables that determine attitudes towards advertising on social media.

V. CONCLUSION

In conclusion, the research model proposed by Chang-Dae Ham [9], when tested on the Instagram social media platform, shows that the only relationship that can show the integration between the persuasion knowledge model (PKM) and protection motivation theory (PMT) is through self-efficacy where the higher of consumers knowledge of persuasion techniques from OBA will further increase consumer self-efficacy and make consumers see that the issue of privacy is not a serious matter and there is no need to try to avoid advertising because they feel sure that it will be easy to overcome the persuasion technique from OBA.

Furthermore, from the results of this study, it can be seen that consumers view the persuasion techniques used by OBA (in this case, the use of covert cookies) only for “positive” purposes as illustrated in the perceived benefits and perceived personalization. And on the other hand, only things that are “negative” such as perceived risk and reactance, will affect protection motivation (privacy concern) and ultimately lead to ad avoidance behavior.

A. Implications of the study

First, this study found that persuasion knowledge from consumers only played a significant role in positive factors such as perceived benefit and self-efficacy (cognitive appraisal) and perceived personalization (cognitive process). These findings are different from the research findings conducted by Chang-dae Ham [9], where persuasion knowledge plays a significant role in all factors in cognitive appraisal but not in cognitive processes. This shows that currently, consumers already have good knowledge about covert persuasion techniques using cookie files by OBA so that consumers can easily control these persuasion techniques and no longer create fear.

Control over the use of cookie files as a covert technique in OBA is also helped because various social media platforms such as Instagram have options in their settings section regarding data sharing. Instagram users can set whether or not they allow their behavioral data to be shared with third parties to provide relevant advertisements. Web browsers such as Google as well as android/iPhone mobile

devices have also enabled their users to clear cookies and their web browsing history. And from the results of this study, it can be seen that consumers already know these ways to control the tracking carried out by OBA.

Second, this study found that negative factors such as perceived risk and reactance played a significant role in privacy and ad avoidance issues in terms of protective motivation and behavior. These negative factors are not at all related to persuasion knowledge, and this shows the consumer's perception that the nature of advertising is intrusive [75] without paying attention to the hidden persuasion of advertising that causes ad avoidance behavior. In the context of advertising on Instagram, the intrusive nature of ads may be caused by too often ads appear, especially when an Instagram user is looking at the Instagram stories section. Because on Instagram stories, a user will see an ad almost every time they finish viewing the stories of two of their friends (two stories one ad). This is certainly felt to interfere with the experience of using Instagram.

Third, this study found that the only connecting factor between PKM and PMT is through self-efficacy, where self-efficacy shows the level of consumer persuasion knowledge and confidence in overcoming covert persuasion techniques from OBA. The higher the self-efficacy of a consumer, the easier it will be for consumers to control OBA persuasion techniques and consider it not a threat to privacy. Thus, the managerial implications that can be drawn from the results of this study are:

First, Considering the results of this study, consumers already have fairly good persuasion knowledge and confidence in controlling OBA persuasion techniques. Marketers and Instagram ad networks must continue to maintain and improve ways of providing clear information about tracking techniques in OBA and maintain giving users choices in sharing their behavioral data on Instagram as it is currently being done. Because by providing clear information and options for sharing behavioral data, it will give consumers more flexibility in controlling OBA, and the more consumers are free to control OBA, the consumers will not view OBA as a threat so that it will reduce ad avoidance behavior.

Second, because consumers still view advertisements as intrusive, marketers and the Instagram ad network have to think more about the number of ads that appear every time a consumer uses Instagram and think about each ad's content. By making advertisements that appear not too massive, consumers on Instagram will not be too disturbed by the appearance of advertisements. About advertising content, relevant advertisements are often not followed by exciting and informative content so that consumers will not easily avoid an advertisement that appears on Instagram. By creating exciting and more informative content, of course, the ad avoidance behavior of consumers on Instagram can be reduced.

This study also has social implications. This study

indicates that only negative factors such as perceived risk and reactance have a significant effect on privacy concern and ad avoidance without having a relationship with the persuasion knowledge of OBA. Apart from the intrusive nature of advertising, these results may also indicate consumer fear on Instagram about the potential for fraud and phishing. False advertisements often also appear in the scope of online ads, which makes consumers afraid to click on an online advertisement that appears, including on social media, because it can put them at risk of dealing with online fraudsters. This risk is very serious and more difficult for consumers to overcome than understanding the use of cookies in OBA. Of course, this needs to be a concern for the government as a policymaker and also for the advertising industry players to do something to protect the interests of consumers.

B. Limitations and future study

This study has several limitations: First, This study only examines respondents aged 18-34 years; by expanding the age range of respondents in the next study, it may provide better validity. Second, This research only examines OBA in the form of videos and image ads within the scope of Instagram, and there are many other forms of OBA found on other platforms such as video ads on YouTube, text ads on Twitter, or banner ads on gaming and movie streaming applications. Researching other platforms might give a better picture of each relationship in this research model.

Third, This research has not included a factor in consumers' ability to control OBA tracking methods such as deleting cookies or using data sharing settings options; future research may include these factors as one of the determinants for testing coping appraisals

REFERENCES

- [1] Hootsuite and We Are Social, "Digital in Indonesia: All the Statistics You Need in 2021," *DataReportal – Global Digital Insights*, Jan. 2021. <https://datareportal.com/reports/digital-2021-indonesia> (accessed Apr. 17, 2021).
- [2] F. J. Zuiderveen Borgesius, "Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation," *Computer Law & Security Review*, vol. 32, no. 2, pp. 256–271, Apr. 2016, doi: 10.1016/j.clsr.2015.12.013.
- [3] A.-R. Jung, "The influence of perceived ad relevance on social media advertising: An empirical examination of a mediating role of privacy concern," *Computers in Human Behavior*, vol. 70, pp. 303–309, 2017, doi: 10.1016/j.chb.2017.01.008.
- [4] S. C. Boerman, S. Kruikemeier, and F. J. Zuiderveen Borgesius, "Online Behavioral Advertising: A Literature Review and Research Agenda," *Journal of Advertising*, vol. 46, no. 3, pp. 363–376, 2017, doi: 10.1080/00913367.2017.1339368.
- [5] T. H. Baek and M. Morimoto, "Stay Away From Me," *Journal of Advertising*, vol. 41, no. 1, pp. 59–76, 2012, doi: 10.2753/joa0091-3367410105.
- [6] A. M. McDonald and L. F. Cranor, *Americans' attitudes about internet behavioral advertising practices*. ACM Press, 2010. doi: 10.1145/1866919.1866929.
- [7] A. Nill and R. J. Aalberts, "Legal and Ethical Challenges of Online Behavioral Targeting in Advertising," *Journal of Current*

- Issues & Research in Advertising*, vol. 35, no. 2, pp. 126–146, 2014, doi: 10.1080/10641734.2014.899529.
- [8] G. van Noort, E. G. Smit, and H. A. M. Voorveld, *The Online Behavioural Advertising Icon: Two User Studies*. Springer Fachmedien Wiesbaden, 2013. doi: 10.1007/978-3-658-02365-2_28.
- [9] C.-D. Ham, “Exploring how consumers cope with online behavioral advertising,” *International Journal of Advertising*, vol. 36, no. 4, pp. 632–658, 2017, doi: 10.1080/02650487.2016.1239878.
- [10] M. Friestad and P. Wright, “The Persuasion Knowledge Model: How People Cope with Persuasion Attempts,” *Journal of Consumer Research*, vol. 21, no. 1, p. 1, 1994, doi: 10.1086/209380.
- [11] R. W. Rogers, “A Protection Motivation Theory of Fear Appeals and Attitude Change,” *The Journal of Psychology*, vol. 91, no. 1, pp. 93–114, 1975, doi: 10.1080/00223980.1975.9915803.
- [12] N. S. Sahni, S. C. Wheeler, and P. Chintagunta, “Personalization in Email Marketing: The Role of Noninformative Advertising Content,” *Marketing Science*, vol. 37, no. 2, pp. 236–258, 2018, doi: 10.1287/mksc.2017.1066.
- [13] D. Shelton, “Online Behavioral Advertising Tracking Users: Gold Mine or Land Mine,” *Landslide*, vol. 5, p. 26, 2012.
- [14] H. Kim and J. Huh, “Perceived Relevance and Privacy Concern Regarding Online Behavioral Advertising (OBA) and Their Role in Consumer Responses,” *Journal of Current Issues & Research in Advertising*, vol. 38, no. 1, pp. 92–105, Jan. 2017, doi: 10.1080/10641734.2016.1233157.
- [15] K. Yang, “Online Behavioral Advertising: Why and how online customers respond to it? : An experimental study into the effects of personalized levels, rewards on click-through intentions towards ads between Chinese and Dutch,” Mar. 13, 2020. <http://essay.utwente.nl/80840/> (accessed Jun. 19, 2021).
- [16] L. J. Helsloot, G. Tillem, and Z. Erkin, “Privacy concerns and protection measures in online behavioural advertising,” in *2017 Symposium on Information Theory and Signal Processing in the Benelux: WIC/SP 2017*, 2017, pp. 89–96.
- [17] A. Matic, M. Pielot, and N. Oliver, “‘OMG! How did it know that?’: Reactions to Highly-Personalized Ads,” in *Adjunct Publication of the 25th Conference on User Modeling, Adaptation and Personalization*, New York, NY, USA, Jul. 2017, pp. 41–46. doi: 10.1145/3099023.3101411.
- [18] M. Eslami, S. R. Krishna Kumaran, C. Sandvig, and K. Karahalios, “Communicating Algorithmic Process in Online Behavioral Advertising,” in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA, Apr. 2018, pp. 1–13. doi: 10.1145/3173574.3174006.
- [19] A. D. Miyazaki, “Online Privacy and the Disclosure of Cookie Use: Effects on Consumer Trust and Anticipated Patronage,” *Journal of Public Policy & Marketing*, vol. 27, no. 1, pp. 19–33, 2008, doi: 10.1509/jppm.27.1.19.
- [20] A. F. Westin, “Special report,” *Communications of the ACM*, vol. 10, no. 9, pp. 533–537, 1967, doi: 10.1145/363566.363579.
- [21] Angst and Agarwal, “Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion,” *MIS Quarterly*, vol. 33, no. 2, p. 339, 2009, doi: 10.2307/20650295.
- [22] N. K. Malhotra, S. S. Kim, and J. Agarwal, “Internet Users’ Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model,” *Information Systems Research*, vol. 15, no. 4, pp. 336–355, 2004, doi: 10.1287/isre.1040.0032.
- [23] S. Ward, K. Bridges, and B. Chitty, “Do Incentives Matter? An Examination of On-line Privacy Concerns and Willingness to Provide Personal and Financial Information,” *Journal of Marketing Communications*, vol. 11, no. 1, pp. 21–40, 2005, doi: 10.1080/1352726042000263575.
- [24] X.-B. Li and S. Sarkar, “Against Classification Attacks: A Decision Tree Pruning Approach to Privacy Protection in Data Mining,” *Operations Research*, vol. 57, no. 6, pp. 1496–1509, 2009, doi: 10.1287/opre.1090.0702.
- [25] K. D. Martin and P. E. Murphy, “The role of data privacy in marketing,” *J. of the Acad. Mark. Sci.*, vol. 45, no. 2, pp. 135–155, Mar. 2017, doi: 10.1007/s11747-016-0495-4.
- [26] D. L. Mothersbaugh, W. K. Foxx, S. E. Beatty, and S. Wang, “Disclosure Antecedents in an Online Service Context: The Role of Sensitivity of Information,” *Journal of Service Research*, vol. 15, no. 1, pp. 76–98, Feb. 2012, doi: 10.1177/1094670511424924.
- [27] J.-Y. Son and S. S. Kim, “Internet Users’ Information Privacy-Protective Responses: A Taxonomy and a Nomological Model,” *MIS Quarterly*, vol. 32, no. 3, pp. 503–529, 2008, doi: 10.2307/25148854.
- [28] L. K. John, A. Acquisti, and G. Loewenstein, “Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information,” *Journal of Consumer Research*, vol. 37, no. 5, pp. 858–873, Feb. 2011, doi: 10.1086/656423.
- [29] H. Xu, H.-H. Teo, B. C. Y. Tan, and R. Agarwal, “Research Note—Effects of Individual Self-Protection, Industry Self-Regulation, and Government Regulation on Privacy Concerns: A Study of Location-Based Services,” *Information Systems Research*, vol. 23, no. 4, pp. 1342–1363, Dec. 2012, doi: 10.1287/isre.1120.0416.
- [30] A. Bleier and M. Eisenbeiss, “The Importance of Trust for Personalized Online Advertising,” *Journal of Retailing*, vol. 91, no. 3, pp. 390–409, Sep. 2015, doi: 10.1016/j.jretai.2015.04.001.
- [31] J. Wirtz and M. O. Lwin, “Regulatory Focus Theory, Trust, and Privacy Concern,” *Journal of Service Research*, vol. 12, no. 2, pp. 190–207, Nov. 2009, doi: 10.1177/1094670509335772.
- [32] P. McCole, E. Ramsey, and J. Williams, “Trust considerations on attitudes towards online purchasing: The moderating effect of privacy and security concerns,” *Journal of Business Research*, vol. 63, no. 9, pp. 1018–1024, Sep. 2010, doi: 10.1016/j.jbusres.2009.02.025.
- [33] J. Phelps, G. Nowak, and E. Ferrell, “Privacy Concerns and Consumer Willingness to Provide Personal Information,” *Journal of Public Policy & Marketing*, vol. 19, no. 1, pp. 27–41, 2000, doi: 10.1509/jppm.19.1.27.16941.
- [34] I. Simonson, “Determinants of Customers’ Responses to Customized Offers: Conceptual Framework and Research Propositions,” *Journal of Marketing*, vol. 69, no. 1, pp. 32–45, Jan. 2005, doi: 10.1509/jmkg.69.1.32.55512.
- [35] T. F. Mangleburg and T. Bristol, “Socialization and Adolescents’ Skepticism toward Advertising,” *Journal of Advertising*, vol. 27, no. 3, pp. 11–21, Oct. 1998, doi: 10.1080/00913367.1998.10673559.
- [36] P. Wright, M. Friestad, and D. M. Boush, “The Development of Marketplace Persuasion Knowledge in Children, Adolescents, and Young Adults,” *Journal of Public Policy & Marketing*, vol. 24, no. 2, pp. 222–233, Sep. 2005, doi: 10.1509/jppm.2005.24.2.222.
- [37] A. Kirmani and M. C. Campbell, “Taking the target’s perspective: The persuasion knowledge model,” *Social psychology of consumer behavior*, pp. 297–316, 2009.
- [38] S. F. Verkijika, “Understanding smartphone security behaviors: An extension of the protection motivation theory with anticipated regret,” *Computers & Security*, vol. 77, pp. 860–870, Aug. 2018, doi: 10.1016/j.cose.2018.03.008.
- [39] J. Wang, B. Liu-Lastres, B. W. Ritchie, and D. J. Mills, “Travellers’ self-protections against health risks: An application of the full Protection Motivation Theory,” *Annals of Tourism Research*, vol. 78, p. 102743, Sep. 2019, doi: 10.1016/j.annals.2019.102743.
- [40] J. Van Ouytsel and K. Ponnet, “Adolescents’ Intent to Engage in Privacy-Protection on Facebook: An Application of the Protection Motivation Theory,” *ICA’s 68th Annual Conference*, 2018. <http://tinyurl.com/y8ano8dy> (accessed Jun. 19, 2021).
- [41] N. Mohamed and I. H. Ahmad, “Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia,” *Computers in Human Behavior*, vol. 28, no. 6, pp. 2366–2375, 2012, doi: 10.1016/j.chb.2012.07.008.
- [42] S. Youn, “Teenagers’ Perceptions of Online Privacy and Coping Behaviors: A Risk–Benefit Appraisal Approach,” *Journal of*

- Broadcasting & Electronic Media*, vol. 49, no. 1, pp. 86–110, 2005, doi: 10.1207/s15506878johem4901_6.
- [43] D. V. SHAH, R. J. FABER, and S. YOUN, “Susceptibility and Severity: Perceptual Dimensions Underlying the Third-Person Effect,” *Communication Research*, vol. 26, no. 2, pp. 240–267, Apr. 1999, doi: 10.1177/009365099026002006.
- [44] K. B. Sheehan and M. G. Hoy, “Dimensions of Privacy Concern among Online Consumers,” *Journal of Public Policy & Marketing*, vol. 19, no. 1, pp. 62–73, 2000, doi: 10.1509/jppm.19.1.62.16949.
- [45] T. B. White, “Consumer Disclosure and Disclosure Avoidance: A Motivational Framework,” *Journal of Consumer Psychology*, vol. 14, no. 1, pp. 41–51, Jan. 2004, doi: 10.1207/s15327663jcp1401&2_6.
- [46] J. V. Baren, W. IJsselstein, N. Romero, P. Markopoulos, and B. Ruyter, “Affective Benefits in Communication: The development and field-testing of a new questionnaire measure,” *Proceedings of PRESENCE*, 2003.
- [47] W. IJsselstein, J. van Baren, P. Markopoulos, N. Romero, and B. de Ruyter, “Measuring Affective Benefits and Costs of Mediated Awareness: Development and Validation of the ABC-Questionnaire,” in *Awareness Systems: Advances in Theory, Methodology and Design*, P. Markopoulos, B. De Ruyter, and W. Mackay, Eds. London: Springer, 2009, pp. 473–488. doi: 10.1007/978-1-84882-477-5_20.
- [48] A. Bandura, W. H. Freeman, and R. Lightsey, “Self-Efficacy: The Exercise of Control,” *Journal of Cognitive Psychotherapy*, vol. 13, no. 2, pp. 158–166, 1999, doi: 10.1891/0889-8391.13.2.158.
- [49] K. Kim and J. Kim, “Third-party Privacy Certification as an Online Advertising Strategy: An Investigation of the Factors Affecting the Relationship between Third-party Certification and Initial Trust,” *Journal of Interactive Marketing*, vol. 25, no. 3, pp. 145–158, 2011, doi: 10.1016/j.intmar.2010.09.003.
- [50] N. J. RIFON, R. LaROSE, and S. M. CHOI, “Your Privacy Is Sealed: Effects of Web Privacy Seals on Trust and Personal Disclosures,” *Journal of Consumer Affairs*, vol. 39, no. 2, pp. 339–362, 2005, doi: 10.1111/j.1745-6606.2005.00018.x.
- [51] X. Zhang, S. Liu, X. Chen, L. Wang, B. Gao, and Q. Zhu, “Health information privacy concerns, antecedents, and information disclosure intention in online health communities,” *Information & Management*, vol. 55, no. 4, pp. 482–493, Jun. 2018, doi: 10.1016/j.im.2017.11.003.
- [52] K. Adhikari and R. K. Panda, “Users’ Information Privacy Concerns and Privacy Protection Behaviors in Social Networks,” *Journal of Global Marketing*, vol. 31, no. 2, pp. 96–110, Mar. 2018, doi: 10.1080/08911762.2017.1412552.
- [53] D. Lee, R. Larose, and N. Rifon, “Keeping our network safe: a model of online protection behaviour,” *Behaviour & Information Technology*, vol. 27, no. 5, pp. 445–454, 2008, doi: 10.1080/01449290600879344.
- [54] W. O. Bearden, D. M. Hardesty, and R. L. Rose, “Consumer Self-Confidence: Refinements in Conceptualization and Measurement,” *Journal of Consumer Research*, vol. 28, no. 1, pp. 121–134, Jun. 2001, doi: 10.1086/321951.
- [55] H. Bang, J. Kim, and D. Choi, “Exploring the effects of ad-task relevance and ad salience on ad avoidance: The moderating role of internet use motivation,” *Computers in Human Behavior*, vol. 89, pp. 70–78, Dec. 2018, doi: 10.1016/j.chb.2018.07.020.
- [56] C.-H. Cho and H. J. Cheon, “WHY DO PEOPLE AVOID ADVERTISING ON THE INTERNET?,” *Journal of Advertising*, vol. 33, no. 4, pp. 89–97, 2004, doi: 10.1080/00913367.2004.10639175.
- [57] J. K. Kim and S. H. Seo, “An Exploration of Advertising Avoidance by Audiences across Media,” *International Journal of Contents*, vol. 13, no. 1, pp. 76–85, 2017, doi: 10.5392/IJoC.2017.13.1.076.
- [58] P. S. Speck and M. T. Elliott, “Predictors of Advertising Avoidance in Print and Broadcast Media,” *Journal of Advertising*, vol. 26, no. 3, pp. 61–76, 1997, doi: 10.1080/00913367.1997.10673529.
- [59] J. W. Brehm, *A theory of psychological reactance*. Oxford, England: Academic Press, 1966, pp. x, 135.
- [60] S. S. Brehm and J. W. Brehm, *Introduction: Freedom, Control, and Reactance Theory*. Elsevier, 1981. doi: 10.1016/b978-0-12-129840-1.50005-3.
- [61] B. D. Rosenberg and J. T. Siegel, “A 50-year review of psychological reactance theory: Do not read this article,” *Motivation Science*, vol. 4, no. 4, pp. 281–300, 2018, doi: 10.1037/mot0000091.
- [62] C. Steindl, E. Jonas, S. Sittenthaler, E. Traut-Mattausch, and J. Greenberg, “Understanding Psychological Reactance,” *Zeitschrift für Psychologie*, vol. 223, no. 4, pp. 205–214, Oct. 2015, doi: 10.1027/2151-2604/a000222.
- [63] M. Puzakova, J. F. Rocereto, and H. Kwak, “Ads are watching me,” *International Journal of Advertising*, vol. 32, no. 4, pp. 513–538, 2013, doi: 10.2501/ija-32-4-513-538.
- [64] C. Li, “When does web-based personalization really work? The distinction between actual personalization and perceived personalization,” *Computers in Human Behavior*, vol. 54, pp. 25–33, Jan. 2016, doi: 10.1016/j.chb.2015.07.049.
- [65] R. E. Crossler, “Protection Motivation Theory: Understanding Determinants to Backing Up Personal Data,” in *2010 43rd Hawaii International Conference on System Sciences*, Jan. 2010, pp. 1–10. doi: 10.1109/HICSS.2010.311.
- [66] S. Dolnicar and Y. Jordaan, “A Market-Oriented Approach to Responsibly Managing Information Privacy Concerns in Direct Marketing,” *Journal of Advertising*, vol. 36, no. 2, pp. 123–149, Jun. 2007, doi: 10.2753/JOA0091-3367360209.
- [67] I. Woon, G.-W. Tan, and R. Low, “A Protection Motivation Theory Approach to Home Wireless Security,” *ICIS 2005 Proceedings*, Dec. 2005, [Online]. Available: <https://aisel.aisnet.org/icis2005/31>
- [68] R. Larose and N. J. Rifon, “Promoting i-Safety: Effects of Privacy Warnings and Privacy Seals on Risk Assessment and Online Privacy Behavior,” *Journal of Consumer Affairs*, vol. 41, no. 1, pp. 127–149, 2007, doi: 10.1111/j.1745-6606.2006.00071.x.
- [69] T. B. White, D. L. Zahay, H. Thorbjørnsen, and S. Shavitt, “Getting too personal: Reactance to highly personalized email solicitations,” *Market Lett*, vol. 19, no. 1, pp. 39–50, Mar. 2008, doi: 10.1007/s11002-007-9027-9.
- [70] S.-M. Hong and S. Faedda, “Refinement of the Hong Psychological Reactance Scale,” *Educational and Psychological Measurement*, vol. 56, no. 1, pp. 173–182, Feb. 1996, doi: 10.1177/0013164496056001014.
- [71] J. F. Hair, W. C. Black, B. J. Babin, and R. E. Anderson, *Multivariate data analysis. vol Book, Whole*. Pearson Education Limited, Harlow, 2014.
- [72] S. Y. Ho, “The Attraction of Internet Personalization to Web Users,” *Electronic Markets*, vol. 16, no. 1, pp. 41–50, Feb. 2006, doi: 10.1080/10196780500491162.
- [73] H.-F. Lin, “Understanding Behavioral Intention to Participate in Virtual Communities,” *CyberPsychology & Behavior*, vol. 9, no. 5, pp. 540–547, Oct. 2006, doi: 10.1089/cpb.2006.9.540.
- [74] H. Nysveen, P. E. Pedersen, and H. Thorbjørnsen, “Intentions to Use Mobile Services: Antecedents and Cross-Service Comparisons,” *Journal of the Academy of Marketing Science*, vol. 33, no. 3, pp. 330–346, Jul. 2005, doi: 10.1177/0092070305276149.
- [75] Y. J. Chung and E. Kim, “Predicting Consumer Avoidance of Native Advertising on Social Networking Sites: A Survey of Facebook Users,” *Journal of Promotion Management*, vol. 27, no. 1, pp. 1–26, Jan. 2021, doi: 10.1080/10496491.2020.1809590.
- [76] C. A. Lin and T. Kim, “Predicting user response to sponsored advertising on social media via the technology acceptance model,” *Computers in Human Behavior*, vol. 64, pp. 710–718, Nov. 2016, doi: 10.1016/j.chb.2016.07.027.