Using Subtle Message Framing to Shift Privacy Decisions

Completed Paper

Da Ma
Zhejiang University
mada_123@zju.edu.cn

Xixian Peng
Zhejiang University
pengxx@zju.edu.cn

Matthew J. Hashim
University of Arizona
mhashim@arizona.edu

Quizhen Wang
Zhejiang University
wqz@zju.edu.cn

ABSTRACT

The design of privacy settings plays a crucial role in the interactions between users and service providers. Our research examines whether, how, and when positive and negative message framing influence users' decision-making in privacy settings via two experimental studies. Study 1 shows that positive framing performs better in persuading users to grant permission requests than negative framing, and the information processing fluency accounts for this effect. Study 2 further identifies the moderating role of privacy salience, that is, the framing effect disappears after enhancing privacy salience. Overall, our research clarifies the impact of message framing on privacy behaviors, reconciles some of the inconsistent findings in framing effects, and suggests a potential way to integrate the normative and behavioral theoretical lens in previous IS privacy research using message framing as an entry point. Our findings also provide guidance for policymakers and practitioners regarding how to frame messages in privacy settings.

Keywords

privacy decisions, heuristics, message framing, information processing fluency, privacy salience

INTRODUCTION

Individuals manage their privacy by granting specific permissions to service providers and, thereby, control their self-disclosure (Adjerid et al. 2019). Self-disclosure can be challenging for individuals due to the hiding of key disclosure information in lengthy privacy policies or intrusive default settings. To combat these issues, regulations such as the General Data Protection Regulation (GDPR) in the European Union[1] and the Personal Information Protection Law (PIPL) in China,[2] require businesses to explain the purpose of data collection and data use to users and obtain explicit consent. Similarly, some firms have taken a proactive approach to the concern such as Apple's implementation of explicit user consent for data collection on iOS devices.[3] Given user privacy concerns and the responses by both regulators and industry, a better understanding of how the design of privacy settings affects users' decision-making is warranted.

Subtle design and wording changes—known as message framing in persuasive design—can have profound impacts on consumers' behaviors (Seo and Park 2019, Seo and Dillard 2019). Message framing refers to constructing the same content of a message into different frames by emphasizing either the benefits afforded by adopting the recommendation, or the costs associated with failing to adopt it (i.e., positive versus negative framing).[4] Message framing has been increasingly used in the design of privacy settings, and after exploring several popular shopping

[1] See https://gdpr-info.eu/.
[2] See http://www.gov.cn/xinwen/2021-08/20/content_5632486.htm.
[3] See https://www.apple.com/ios/ios-14/.
[4] We follow the definition of "goal framing" by Levin et al. (1998), in which the outcome of a recommended behavior is framed, as frequently applied in the persuasion literature. A detailed discussion on our specific focus of message framing is in the subsection of the literature review (2.2).

apps, we found that positive versus negative message framing differs not only between providers but also within the same provider at different times. For example, in January 2021, the privacy settings of JD.com[5] described permission requests by emphasizing the benefits of granting permission (positive framing), whereas Pinduoduo adopted negative framing, emphasizing the potential costs of non-authorization for the same permission request. However, five months later, the message framing strategies for these apps were reversed entirely, with Pinduoduo employing positive framing and JD.com using negative framing. Our observation implies that firms are interested in understanding the effects of message framing on users' privacy behaviors, but do not understand the impact or effectiveness of their designs.

The dominant focus of previous literature on individuals' privacy behaviors has been on the rational-based analytical privacy calculus process, which assumes that users' privacy setting decisions are determined by the deliberate trade-off between privacy costs and benefits. However, the intuition-based heuristic process, such as the influence of heuristics and decision biases, has been largely neglected (Dinev et al. 2015, Adjerid et al. 2019). Accordingly, it is unclear how users' privacy settings will be affected by message framing—a heuristic factor—and how to explain the impact. Further, although message framing has been widely used in contexts such as healthcare, retailing, and advertising (Kahneman and Tversky 1979, Scheufele and Iyengar 2014), the existing findings are difficult to apply to privacy-related decisions. It is unclear which type of framing is most persuasive and influences expected behaviors (O'Keefe and Jensen 2006, Xiao

[5] JD.com and Pingduoduo are two leading e-commerce companies in China.

and Benbasat 2015, Karlan et al. 2016). Besides, substantial studies indicate that the framing effect varies greatly across contexts (Levin et al. 1998, Cesario et al. 2013, Adjerid et al. 2019). Thus, previous findings are insufficient to account for whether and how message framing influences users' permission-granting behavior in privacy settings.

These theoretical research gaps, along with the practical use of message framing in privacy settings, motivates us to investigate the role of message framing in privacy decision-making. Specifically, we aim to answer the following questions: 1) Will subtle differences in message framing (positive versus negative) impact users' behaviors? If so, which type is more effective in persuading users to grant permissions? 2) What are the underlying mechanisms, including how to interpret the different impacts between positive versus negative message framing (mediating effect)? Is there a boundary condition (moderator) for the framing effect?

To address these questions, we develop an m-commerce application and conduct two experimental studies. In study 1, we manipulate the framing of the message presented in the privacy permission settings and capture users' actual privacy behavior and decision process information such as response time. We empirically find that framing the privacy permission request in a positive (versus negative) way encourages people to grant privacy permissions. Further, intuitive-based processing fluency, rather than the rational-based privacy calculus, mediates this framing effect in privacy decision-making. In study 2, drawing on the theoretical lens of dual-process models, we further manipulate privacy salience in addition to message framing. The results replicate the main effect of message framing and show a moderating effect

of privacy salience. That is, the framing effect disappears after enhancing privacy salience, providing support for the analytical-based privacy calculus.

These findings contribute to the IS literature on explaining and predicting user privacy decision-making. First, the discovery of the different effects between positive and negative message framing on users' privacy settings provides evidence for the emerging behavioral perspective in privacy research. Next, we reveal the underlying mechanism and boundary conditions for the influence of such heuristic factors on privacy behaviors from the information processing perspective. Our discussion of decision processes further suggests that the traditional normative and nascent behavioral paths may influence individual privacy behavior simultaneously and independently of each other, providing a way to integrate the two core theoretical lenses in the IS privacy literature. Such findings contribute to the framing effect literature as well, by not only extending it to the privacy domain, but also by identifying the preconditions for message framing to play a role in user privacy decision-making, reconciling some of the previously-found inconsistent findings. Practically, the discussion on the effectiveness of positive versus negative message framing provides pragmatic implications for policymakers and online service providers.

RELATED LITERATURE

Privacy Decision-Making

Users' privacy decision-making is an important research topic in the IS domain (Smith et al. 2011, Belanger and Crossler 2019) that has attracted continued attention from researchers

because of the ever-changing privacy policies (e.g., GDPR) and businesses' updates in privacy settings to comply with said regulations (e.g., Apple's App Tracking). There are two primary research perspectives in the IS privacy literature (Dinev et al. 2015, Adjerid et al. 2018). The dominant view holds the normative perspective that individuals are economically rational and make utility-maximizing privacy choices (Dinev et al. 2015). In line with this view, substantial studies have adopted rational calculus grounded theories (Laufer and Wolfe 1977) to examine the factors influencing users' privacy decision-making (Smith et al. 2011, Al-Natour et al. 2020). The basic idea of privacy calculus is that users' decisions are driven by a systematic weighting of the potential privacy risks and anticipated benefits induced by privacy information disclosure (Dinev and Hart 2006, Cavusoglu et al. 2016).

Besides the normative perspective, some have highlighted a behavioral perspective and argued factors unrelated to the privacy calculus might also influence users' behaviors. For instance, people are more likely to disclose personal information when the same privacy-related questions are presented in a decreasing (vs. an increasing) order of intrusiveness (Acquisti et al. 2012). The "default option" can also nudge decision-making such that users assigned to the shared-by-default condition have a higher sharing tendency than those assigned to the private-by-default condition (Cho et al. 2019). Users also show a higher willingness to pay for privacy-enhanced features when privacy protection is set as a default (Dogruel et al. 2017). This stream of research seems to question traditional IS privacy research, but it also opens up a new research direction to enhance our understanding and prediction of user privacy behavior. In our research,

we consider positive versus negative message framing on individual privacy settings as the entry point to extend the behavioral perspective of privacy research.

Message Framing

Many consider prospect theory as the most influential framework for conceptualizing message framing (Kahneman and Tversky 1979). Given its theoretical and practical importance, message framing has been a fixture in the previous literature for over four decades, and its definition and operation have been developed and extended to diverse areas. As a result, there exist different framing levels that apply to distinct research situations (as discussed by Cesario et al. (2013)), which is also considered to be an important reason for the high inconsistency and low comparability of existing research findings (Scheufele and Iyengar 2014, Liu and Scheufele 2016). As called for by Carnahan et al. (2019), we focus on the original definition of "goal framing," which requires that the message communicated remains the same and only varies in framing (Levin et al. 1998, Nabi et al. 2020). Specifically, in privacy settings, positive framing refers to positive outcomes from granting permission, and negative framing suggests the absence of positive outcomes from denying permission (Seo and Dillard 2019).

Although the difference is subtle, positive versus negative message framing could profoundly affect individuals' decision-making (Scheufele and Iyengar 2014). Over the last decades, the framing effect has been documented in many fields, such as health advocacy (Rothman and Salovey 1997, Ainiwaer et al. 2021), marketing campaigns (Xiao and Benbasat 2015), IT security (Anderson and Agarwal 2010), and environmental protection (Bilandzic et al.

2017). However, the effectiveness of the two kinds of message framing in the context of privacy is still subject to debate, as previous findings regarding which kind of framing in a persuasive message is more effective are inconsistent (Cesario et al. 2013). For instance, a meta-analysis by O'Keefe and Jensen (2006) showed that positive framings are more persuasive in the disease prevention context. In contrast, Xiao and Benbasat (2015) found that the negative framing is more effective in influencing consumers' responses to product recommendations. Karlan et al. (2016) even suggested that message framings do not have significant effects on clients' savings behavior. Additionally, prior studies indicate that the impacts of message framing are highly relevant to the problem domain (Levin et al. 1998, Adjerid et al. 2019). Therefore, the extant literature is unclear on providing guidance for suggested privacy practices.

THEORETICAL FRAMEWORK AND HYPOTHESIS DEVELOPMENT

The debate between normative and behavioral perspectives in privacy is essential because the perspectives are predicated on assumptions about the information-processing mechanisms used in privacy decision-making (Dinev et al. 2015) and correspond with dual-process models from cognitive psychology. These theories suggest that human problem-solving and decision-making are not always purely rational via the deliberate brain (System 2) due to cognitive limitations. In many cases, people rely on the automatic brain (System 1) to use various heuristics that enable them to solve problems and make judgments quickly and efficiently (Evans 2008, Kahneman 2011). Therefore, we derive the influence of positive versus negative framing on users' privacy settings from intuitive judgment (information processing fluency) and consider privacy salience

as the critical boundary factor. The conceptual framework is summarized in Figure 1.

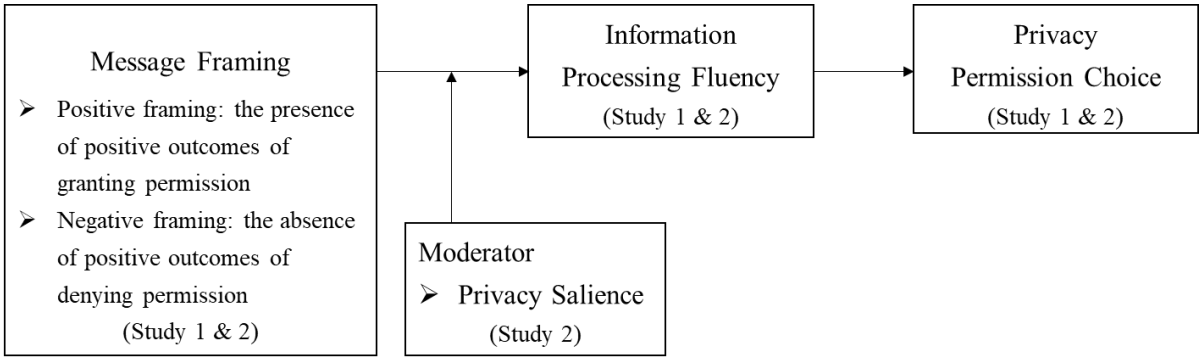

Figure 1. Conceptual Framework

Effects of Message Framing on Privacy Decision-making

Privacy contexts are becoming more complex (Buckman et al. 2019), the information asymmetry between users and businesses in terms of how the data is collected and processed is increasingly prominent (Acquisti et al. 2015), and privacy decision-making often involves a high level of uncertainty (Al-Natour et al. 2020). Moreover, users may put relatively fewer cognitive resources in complex privacy scenarios because they often face other immediate needs and lack specialized privacy knowledge (Kokolakis 2017, Crossler and Belanger 2019). According to prior studies on message framing, the situations where framing effects have been consistently found or even exacerbated have common features such as the context having higher ambiguity or devoting less cognitive effort (Schoorman et al. 1994, Scheufele and Iyengar 2014). Thus, we suggest that the framing effect may be particularly relevant to privacy decisions. Next, we explain how positive versus negative message framings will alter users' permission-granting behavior.

Dual-process theories suggest that when an immediate decision is required and knowledge

and cognitive resource are lacking, people are prone to rely on the intuitive-based judgment path (System 1) to solve problems and make decisions quickly and efficiently (Evans and Curtis-Holmes 2005, Liu et al. 2019). In this path, the most direct and significant manifestation is the degree of processing fluency, referring to the ease or difficulty of processing external stimuli (Schwarz 2004). For example, some stimuli may elicit people to give positive responses unconsciously, such as a better aesthetic experience (Reber et al. 2004), higher brand acceptance (Xu et al. 2014), and greater advertisement persuasiveness (Ku and Chen 2020), simply by triggering a higher degree of processing fluency. These findings suggest further exploration of the effects of message framing on privacy behaviors from an information processing perspective.

We focus on the context of privacy settings and propose that a privacy permission request with positive framing may introduce higher processing fluency than one with negative framing due to the match between message framing and the outcomes of recommended privacy action (Winkielman et al. 2012). Previous studies have found that information would be faster and easier to process if presented in matched semantic forms (Bock et al. 2013, Schwarz et al. 2021). A general principle of such cognitive matches is the valence rule, that is, message elements with the same valence are often matched (Douce et al. 2014, Seo and Dillard 2019). In a typical privacy permission request, there are two message elements: outcomes of the recommended action and message framing. The valence of the recommended action's outcomes is usually positive, such as sales promotion and personalization, as service providers hope that users will grant their permission requests, enabling them to provide better services. Accordingly, the

positive framing may better match the valence of the recommended action's outcomes because it emphasizes the reception of potential benefits; in contrast, the negative framing is less matched. Therefore, we believe that positive framing will enhance processing fluency more than negative framing when users process messages requesting privacy permission.

Next, we turn to how processing fluency will affect individuals' choices on privacy permissions. Schwarz et al. (2021) reviewed previous studies and identified two primary mechanisms underlying the influence of processing fluency on consumers' decisions: 1) fluency-affect link, whereby processing fluency is always marked and experienced as positive (Winkielman et al. 2012); and 2) fluency-familiarity-trust link, whereby processing fluency is sufficient to elicit trust (Silva et al. 2017). In IS privacy research, both positive affect and trust are crucial factors for users to disclose their personal information (Dinev and Hart 2006, Anderson and Agarwal 2011, Lin and Armstrong 2019). Thus, given the associated higher level of information processing fluency, positive message framing may facilitate permission granting in privacy settings more than negative framing. Therefore, we posit the following hypotheses:

H1: When the privacy permission request message is framed positively (versus negatively), users are more likely to grant the permission.

H2: Information processing fluency mediates the effect of message framing on users' permission-granting decisions.

Boundary of the Framing Effect: Privacy Salience

The derivation of the above framing effect mainly relies on the system 1 path in dual-process

theories. The reality is that users are less conscious of privacy and do not put enough cognitive resources into message framings in their privacy settings (Dinev et al. 2015, Acquisti et al. 2017). However, this status is likely to be disrupted by highlighting the "privacy" property of decisions because explicit privacy is a sensitive and attention-introducing issue, and consumers do care about online privacy (Acquisti et al. 2020). Therefore, we vary the degree of privacy salience to explore the boundary of the observed framing effect in privacy settings.

Privacy salience refers to "whether informational privacy is prominent in a person's awareness" (Williams et al. 2016). Research has demonstrated that privacy salience can increase individuals' privacy awareness (Buckman et al. 2019), in turn making them use more cognitive resources to consciously consider their decisions related to privacy (Tsai et al. 2011). As a result, privacy salience can reduce unwise privacy behaviors (Williams et al. 2016). Accordingly, with enhanced privacy salience, people may devote more cognitive effort and mainly rely on the rational-based analytical path to process the permission request message. As positive versus negative framings only change the presentation format but not the core meaning (Scheufele and Iyengar 2014), we propose that under the condition of high privacy salience, users' privacy settings are less susceptible to different message framings. This notion is also consistent with previous findings. For instance, Takemura (1994) found that, when requiring participants to record their decision-making process carefully, the message framing effects disappeared; Septiari (2020) demonstrated that positive versus negative message framings have no difference in influencing human response when the message is labeled salient warning. Thus, we hypothesize:

H3: The effect of message framing on a permission-granting decision is less likely to occur when privacy salience is enhanced.

OVERVIEW OF STUDIES

To examine the proposed hypotheses, we developed a mobile online shopping application and conducted two experimental studies. In Study 1, we tested whether positive versus negative message framing would alter participants' permission-granting decisions (H1) and the mediating effect of processing fluency (H2). Study 2 attempted to replicate the findings of Study 1 and explore the boundary of the message framing effect in privacy settings by examining the moderating effect of privacy salience (H3).

STUDY 1

Design

Study 1 was conducted in the context of Identifier for Advertisers (IDFA),[6] a new privacy setting about app tracking launched in the latest iOS 14.5 by Apple. While IDFA enables marketers to deliver more personalized recommendations, it also brings increasing privacy concerns for users. Thus, how users respond to this new tracking permission request has roused wide attention and discussion in the industry. Study 1 employed a one-factor between-subjects experimental design to examine whether message framing (positive versus negative framing) of IDFA permission requests would influence users' opt in decision.

[6] IDFA is a random device identifier assigned by Apple to a user's device. Advertisers use this to track data and deliver customized advertising. Apple's privacy improvement is about the setting of IDFA permission.

Following previous studies (Scheufele and Iyengar 2014, Liu and Scheufele 2016), we designed two versions of IDFA permission request messages. The positively framed version highlighted the benefits introduced by opting into IDFA, while the negatively framed one outlined that users would miss out on the same benefits if they denied the request. As such, we only changed the framing of the messages, while keeping the objective meanings the same in both. To determine the specific words and sentences used in request messages, we surveyed actual messages employed in the privacy settings of popular mobile online shopping apps (e.g., JD.com, Pingduoduo, etc.). Accordingly, the two versions of messages were designed as follows: "Opting in the IDFA permission, you will receive the personalized services and help you find information of interest" (positive framing), and "Denying the IDFA permission, you will lose the personalized services and miss the information of interest" (negative framing).

Participants and Procedure

We recruited students from a large university in China as participants. To ensure realism, we informed participants that we were conducting a joint research collaboration with an e-commerce company and that they were invited to take part in an internal test of the company's new online shopping app. Participants were required to have at least two years of experience using mobile apps. Those who took part in the pre-test were excluded. Sixty-six qualified participants attended our experiment in exchange for 10 RMB for their time and effort. Participants were randomly assigned to the two experimental conditions. Due to cases of dyslexia among some subjects and inconsistent results between actual choice and post-test, four responses were eliminated, leaving

62 valid observations (41 females, average age =22.03).

After the participants entered our behavioral laboratory, we informed them of the procedure of our study. Only with a clear understanding of our study procedure and after signing the participant consent form, could participants start the experiment. Participants were told that they could browse and use our new shopping app freely just as what they would with other apps. About 2 seconds after opening the app, a message of IDFA permission request would pop up. Participants then needed to make their own decisions about whether they would grant or deny the permission request before continuing to use the app. Overall, the experimental procedure was largely in line with actual mobile app use, during which a pop-up of privacy settings would appear immediately and require users to make choices when they used the app for the first time. We explained the true purpose of the experiment to participants once the study was completed and they were given the opportunity to opt-out of the study if they desired.

Measures

The data set we used in our analysis contains (1) real-time data recorded by our app and (2) self-reported data from a post-task questionnaire. During the main experiment, our app automatically recorded participants' responses and behaviors. First, participants' actual choices for the IDFA permission in the privacy settings were the primary dependent variable. Second, consistent with prior research, we used participants' response time (RT) as an objective and an effective indicator of processing fluency (Leonhardt et al. 2015, Schwarz et al. 2021). We recorded the time duration between the appearance of the privacy setting and the participants' decision about the

privacy permission as the measure of processing fluency.

Data Analysis and Results

The Direct Impact of Message Framing

We first examined the main effect of message framing (positive versus negative) on users' permission-granting decisions in privacy settings. We calculated the rate of permission granting in each condition and found support for H1: in the positive message framing condition, the rate of permission granting was 76.5%, and it decreased to 46.4% in the negatively framed condition (Fisher's exact *p*-value = 0.019).

Variables	**Permission Granting (1=Grant, 0=Deny)**		
	(1)	**(2)**	**(3)**
PositiveFrame	1.322* (0.554)	1.327* (0.555)	1.503* (0.599)
Age		-0.005 (0.080)	0.028 (0.090)
Gender		-0.124 (0.586)	0.050 (0.613)
Liking			0.050 (0.322)
Familiarity			0.738* (0.363)
Constant	-0.143 (0.379)	-0.004 (1.824)	-2.357 (2.216)
Observations	62	62	62
Note: Robust standard errors in parentheses. *$p < 0.05$; **$p < 0.01$; ***$p < 0.001$.			

Table 1. Framing Effects on Permission Granting in Privacy Settings (Study 1)

We also conducted binary logistic regression analyses to examine the effect of message framing (see Table 1). The dependent variable is the privacy permission granting dummy that takes the value of 1 when participants grant the IDFA permission. The variable *PositiveFrame* is an indicator of the independent variable (message framing) that takes the value of 1 if participants were assigned to the positive framing group. The results revealed that presenting a message through positive framing significantly increased the likelihood of privacy permission-granting behaviors from users in privacy settings (β = 1.322, p = 0.017). The effect remained

consistent when considering the control variables of demographics, the degree to which participants liked the app, and familiarity with IDFA permission. Thus, H1 was supported.

Mediating Effect of Processing Fluency

To test the underlying mechanism of the message framing effect, we performed a mediation analysis following Hayes (2017) (PROCESS Model 4, 5000 bootstrapped samples), with message framing as the independent variable, information processing fluency as the mediator, and users' privacy permission choices as the dependent variable. The results revealed a significant indirect effect of message framing on permission-granting behavior through information processing fluency (β = 0.484, SE=0.351, 95% CI = [0.019, 1.368]), supporting H2. Specifically, positive (versus negative) framing increased participants' processing fluency (β = 1.983, p = 0.039) which, in turn, enhanced the likelihood of permission granting (β = 0.244, p = 0.012).

STUDY 2

Study 2 was designed for two purposes. First, we aimed to reaffirm the findings of the effect of message framing on privacy decision-making as well as the mediating effect of information processing fluency observed in Study 1. Taking one step further, we also sought to examine the boundary of the message framing effect: whether enhanced privacy salience would mitigate the impact of message framing on individuals' permission-granting decisions (H3).

Design and Procedure

Study 2 adopted a 2 (framing: positive vs. negative) × 2 (salience: low vs. high) between-

subject experimental design. The manipulation of message framing was identical to Study 1. We manipulated privacy salience by varying the label ("Privacy Settings" versus "Settings") of the permission request pop-up for several theoretical and practical reasons. First, previous studies have consistently shown that the variations in labels can significantly attract users' attention and increase their consciousness (McGarty and Penny 1988, Grebe 2019). In the context of privacy decision-making, Adjerid et al. (2019) have demonstrated that the minor change from the label of "Settings" to "Privacy Settings" could significantly increase users' privacy concerns. Also, from the practical perspective, our survey on current privacy practices suggested that companies have adopted varying labels in permission request pop-ups. For instance, in the JD app, privacy-relevant permissions like Photos and Contacts are presented under the "Privacy Settings" label. Conversely, these privacy permissions are presented under the "Settings" label in the Pinduoduo app. Therefore, grounded in previous research and current privacy practices, we enhanced privacy salience by varying the label of privacy permission from "Settings" to "Privacy Settings."

One hundred twenty-three students from a large university in China were recruited as participants. Three responses were eliminated in the data-screening process, leaving 120 valid observations (78 females, average age =22.50). The experimental scenario, task, and procedure were the same as in Study 1. Participants were randomly assigned to one of the four conditions to complete the app evaluation task. Their choices and response time to the privacy permission request were recorded by our app, and they were required to complete a post-task questionnaire.

Data Analysis and Results

Moderation Analysis

We conducted a binary logistic regression to test the main effect of message framing on permission-granting decisions and the moderating effect of privacy salience (as shown in Table 2). The variable *PrivacySalience* is an indicator variable that takes the value of 1 if participants were assigned to the "Privacy Setting" group. The results reconfirmed that participants in the positive framing treatment were more likely to grant their privacy permission (β = 1.278, p = 0.002), and H1 was again supported. In addition, the interaction between message framing and privacy salience was significant (β = -2.072, p = 0.020). These effects remained consistent after adding control variables.

Variables	Permission Granting (1=Grant, 0=Deny)			
	(1)	(2)	(3)	(4)
PositiveFrame	1.278** (0.408)	2.465*** (0.711)	2.508*** (0.717)	2.670*** (0.743)
PrivacySalience	-0.183 (0.401)	0.617 (0.527)	0.679 (0.554)	0.572 (0.574)
PositiveFrame*PrivacySalience		-2.072* (0.892)	-2.234* (0.921)	-2.455** (0.961)
Age			-0.085 (0.088)	-0.105 (0.090)
Gender			0.441 (0.466)	0.669 (0.503)
Liking				0.508* (0.219)
Familiarity				0.008 (0.209)
Constant	0.124 (0.327)	-0.268 (0.368)	1.470 (2.052)	-0.470 (2.258)
Observations	120	120	120	120
Note: Robust standard errors in parentheses. *p < 0.05; **p < 0.01; ***p < 0.001.				

Table 2. Study 2 Results

Pairwise comparisons (see Figure 2) showed that the proportion of privacy permission granting was significantly higher under the low-level privacy salience condition in positive framing (90.0%) in comparison to negative framing (43.3%; β = 2.465, p = 0.001). However, the difference was not significant when enhancing privacy salience (67.7% versus 58.6%; β = 0.394,

p = 0.465). Thus, H3 was supported.

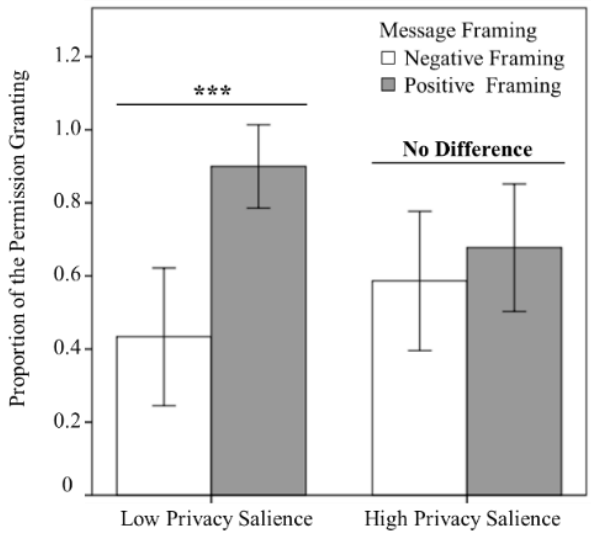

Figure 2. Pairwise Comparisons Results

Mediated Moderation Analysis

We further performed a mediated moderation analysis, following Hayes (2017) (PROCESS Model 8, 5000 bootstrapped samples), with users' choices of privacy permission as the dependent variable, message framing as the independent variable, information processing fluency as the mediator, and privacy salience as the moderator. The results (see Figure 3) revealed that the interaction of message framing and privacy salience significantly influenced information processing fluency (β = -2.615, p = 0.010), which in turn impacted the final permission-granting decisions (β = 0.240, p = 0.004). The indirect effect through information processing fluency was positive and significant when privacy salience was low (β= 0.535, 95% CI = [0.121, 1.221]). In contrast, with enhanced privacy salience, the mediating effect of processing fluency disappeared (β = -0.092, 95% CI = [-0.505, 0.233]). The mediation role of

information processing fluency and the moderation effect of privacy salience were significant, providing evidence for H2 and H3.

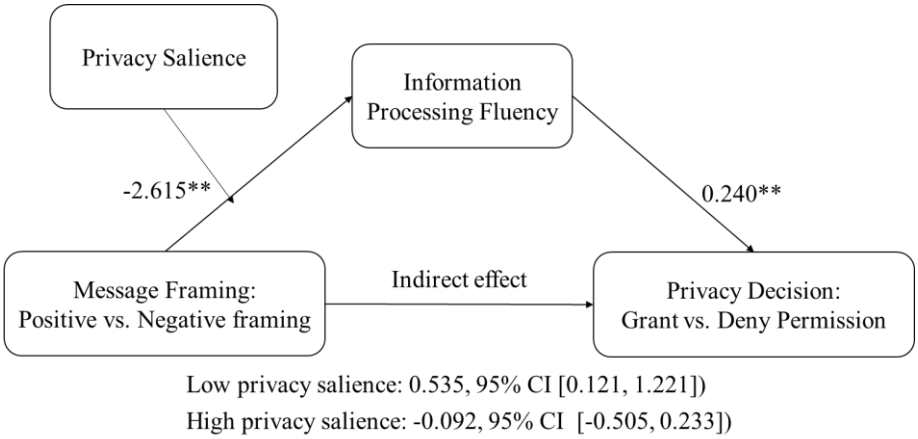

Figure 3. Mediated Moderation Results

DISCUSSION AND CONCLUSION

Message framing is a key construct of heuristics in the psychology, marketing, and IS literature. In the context of privacy settings, although message framing is often an inevitable element in structuring privacy permission request messages, the effects on privacy decision-making are underexplored. Drawing on the theories of dual-process models, we investigated the effect of message framing on users' permission-granting decisions in a privacy setting through two experimental studies. The major findings can be summarized as follows.

The results of the two experimental studies consistently suggested that participants were more likely to choose the "Grant" option when permission requests were framed in a positive (versus negative) way. Our mediation analysis showed that enhanced processing fluency accounted for the outperformed effect of positive framing over negative framing in persuading

participants to grant privacy permissions. In Study 2, we also found that enhancing privacy salience by simply replacing the label of "Settings" with "Privacy Settings," could mitigate the message framing effect. This finding reveals that the effect of heuristics, such as message framing, in the privacy decision context, is contingent upon the degree of privacy salience that people perceive during an event.

Our work contributes to the literature on privacy by increasing our understanding of the impacts of an essential heuristic–message framing–on privacy decision-making. In particular, we have advanced the privacy decision-making literature by discussing the role of message framing and, more importantly, the boundary condition of privacy salience, which has contributed to a more refined and complete understanding of the phenomenon by integrating the normative and behavioral perspectives suggested by previous privacy research.

We also contribute to the growing debate on message framing. Specifically, when privacy salience is relatively low, message framing is processed as a type of heuristic through intuitive judgment (System 1). In this scenario, positive framing matches with the outcomes of recommended action (granting the permission) better and, as a result, leads to greater processing fluency that, further, causes more individuals to grant permission. Consistently, after increasing the level of privacy salience, people are less susceptible to heuristics and the effect of message framing disappears as it does not change the core content of the message. Our results thereby link several streams of research concerning message framing (Levin et al. 1998), dual-process theories (Kahneman 2011), and processing fluency (Schwarz et al. 2021).

REFERENCES

Acquisti A, Brandimarte L, Loewenstein G (2015) Privacy and human behavior in the age of information. *Science* 347(6221):509-514.

Acquisti A, Brandimarte L, Loewenstein G (2020) Secrets and Likes: The Drive for Privacy and the Difficulty of Achieving It in the Digital Age. *J. Consum. Psychol.* 30(4):736-758.

Acquisti A, John LK, Loewenstein G (2012) The Impact of Relative Standards on the Propensity to Disclose. *J. Mark. Res.* 49(2):160-174.

Acquisti A, Adjerid I, Balebako R, Brandimarte L, Cranor LF, Komanduri S, Giovanni Leon P, et al. (2017) Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online. *Acm Computing Surveys* 50(3):1-41.

Adjerid I, Acquisti A, Loewenstein G (2019) Choice Architecture, Framing, and Cascaded Privacy Choices. *Management Science* 65(5):2267-2290.

Adjerid I, Peer E, Acquisti A (2018) Beyond the Privacy Paradox: Objective Versus Relative Risk in Privacy Decision Making. *MIS Quarterly* 42(2):465-488.

Ainiwaer A, Zhang S, Ainiwaer X, Ma F (2021) Effects of Message Framing on Cancer Prevention and Detection Behaviors, Intentions, and Attitudes: Systematic Review and Meta-analysis. *J. Med. Internet Res.* 23(9):e27634.

Al-Natour S, Cavusoglu H, Benbasat I, Aleem U (2020) An Empirical Investigation of the Antecedents and Consequences of Privacy Uncertainty in the Context of Mobile Apps. *Information Systems Research* 31(4):1037-1063.

Anderson CL, Agarwal R (2010) Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Q.* 34(3):613-643.

Anderson CL, Agarwal R (2011) The Digitization of Healthcare: Boundary Risks, Emotion, and Consumer Willingness to Disclose Personal Health Information. *Inf. Sys. Res.* 22(3).

Belanger F, Crossler RE (2019) Dealing with digital traces: Understanding protective behaviors on mobile devices. *J. strateg. inf. syst.* 28(1):34-49.

Bergkvist L, Rossiter JR (2009) Tailor-made single-item measures of doubly concrete constructs. *Int. J. Advert.* 28(4):607-621.

Bilandzic H, Kalch A, Soentgen J (2017) Effects of goal framing and emotions on perceived threat and willingness to sacrifice for climate change. *Sci. Commun.* 39(4):466-491.

Bock TD, Pandelaere M, Kenhove PV (2013) When colors backfire: The impact of color cues on moral judgment. *J. Consum. Psychol.* 23(3):341-348.

Buckman JR, Bockstedt JC, Hashim MJ (2019) Relative Privacy Valuations Under Varying Disclosure Characteristics. *Information Systems Research* 30(2):375-388.

Carnahan D, Hao Q, Yan X (2019) Framing methodology: A critical review. Redlawsk DP, ed. *Oxford Research Encyclopedia of Politics* (Oxford University Press).

Cavusoglu H, Phan TQ, Cavusoglu H, Airoldi EM (2016) Assessing the Impact of Granular Privacy Controls on Content Sharing and Disclosure on Facebook. *Information Systems*

Research 27(4):848-879.

Cesario J, Corker KS, Jelinek S (2013) A self-regulatory framework for message framing. *J. Exp. Soc. Psychol.* 49(2):238-249.

Cho HC, Roh S, Park B (2019) Of promoting networking and protecting privacy: Effects of defaults and regulatory focus on social media users' preference settings. *Comput. Hum. Behav.* 101:1-13.

Crossler RE, Belanger F (2019) Why Would I Use Location-Protective Settings on My Smartphone? Motivating Protective Behaviors and the Existence of the Privacy Knowledge-Belief Gap. *Inf. Syst. Res.* 30(3):995-1006.

Dinev T, Hart P (2006) An extended privacy calculus model for E-commerce transactions. *Inf. Syst. Res.* 17(1):61-80.

Dinev T, McConnell AR, Smith HJ (2015) Informing Privacy Research Through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the "APCO" Box. *Information Systems Research* 26(4):639-655.

Dogruel L, Joeckel S, Vitak J (2017) The valuation of privacy premium features for smartphone apps: The influence of defaults and expert recommendations. *Comput. Hum. Behav.* 77.

Douce L, Janssens W, Swinnen G, Cleempoel KV (2014) Influencing consumer reactions towards a tidy versus a messy store using pleasant ambient scents. *J. Env.Psy.* 40:351-358.

Evans JSB (2008) Dual-processing accounts of reasoning, judgment, and social cognition. *Annu. Rev. Psychol.* 59:255-278.

Evans JSB, Curtis-Holmes J (2005) Rapid responding increases belief bias: Evidence for the dual-process theory of reasoning. *Think Reasoning* 11(4):382-389.

Grebe EH (2019) Actively Creating A Health-Conscious Lifestyle Through Food Label Literacy in Hawaii. Unpublished master dissertation, University of Hawai'i at Manoa.

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

Kahneman D (2011) *Thinking, fast and slow* (Macmillan, New York).

Kahneman D, Tversky A (1979) Prospect theory: analysis of decision under risk. *Econometrica* 47(2):263-291.

Karlan D, McConnell M, Mullainathan S, Zinman J (2016) Getting to the Top of Mind: How Reminders Increase Saving. *Manage. Sci.* 62(12):3393-3411.

Kokolakis S (2017) Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Comput. Secur.* 64:122-134.

Ku H-H, Chen M-J (2020) Promotional phrases as analogical questions: inferential fluency and persuasion. *Eur. J. Market.* 54(4):713-739.

Laufer RS, Wolfe M (1977) Privacy as a concept and a social issue: A multidimensional developmental theory. *J. Soc. Issues* 33(3):22-42.

Leonhardt JM, Catlin JR, Pirouz DM (2015) Is your product facing the ad's center? Facing direction affects processing fluency and ad evaluation. *J. Advert.* 44(4):315-325.

Levin IP, Schneider SL, Gaeth GJ (1998) All frames are not created equal: A typology and critical analysis of framing effects. *Organ. Behav. Hum. Decis. Process.* 76(2):149-188.

Lin S, Armstrong DJ (2019) Beyond Information: The Role of Territory in Privacy Management Behavior on Social Networking Sites. *J. Assoc. Inf. Syst.* 20(4):434-475.

Liu J, Scheufele DA (2016) A revisionist perspective on framing effects. *Oxford Research Encyclopedia of Politics* (Oxford University Press, New York).

Liu Z, Wang X, Min Q, Li W (2019) The effect of role conflict on self-disclosure in social network sites: An integrated perspective of boundary regulation and dual process model. *Inf. Syst. J.* 29(2):279-316.

McGarty C, Penny R (1988) Categorization, accentuation and social judgement. *Br. J. Soc. Psychol.* 27(2):147-157.

Nabi RL, Walter N, Oshidary N, Endacott CG, Nichols JL, Lew Z, Aune A (2020) Can emotions capture the elusive gain-loss framing effect? A meta-analysis. *Com. Res.* 47(8):1107-1130.

O'Keefe D, Jensen JD (2006) The Advantages of Compliance or the Disadvantages of Noncompliance? A Meta-Analytic Review of the Relative Persuasive Effectiveness of Gain-Framed and Loss-Framed Messages. *Commun. Yearb.* 30(1):1-43.

Privacy Europe-International Network (PEIN) General Data Protection Regulation. Accessed July 25th, 2021, https://gdpr-info.eu/.

Reber R, Schwarz N, Winkielman P (2004) Processing fluency and aesthetic pleasure: Is beauty in the perceiver's processing experience? *Pers. Soc. Psychol. Rev.* 8(4):364-382.

Rothman AJ, Salovey P (1997) Shaping perceptions to motivate healthy behavior: the role of message framing. *Psychol. Bull.* 121(1):3-19.

Scheufele DA, Iyengar S (2014) The state of framing research: A call for new directions. *The Oxford Handbook of Political Communication Theories* (Oxford University Press, NY)

Schoorman FD, Mayer RC, Douglas CA, Hetrick CT (1994) Escalation of commitment and the framing effect: An empirical investigation. *J. Appl. Soc. Psychol.* 24(6):509-528.

Schwarz N (2004) Metacognitive experiences in consumer judgment and decision making. *J. Consum. Psychol.* 14(4):332-348.

Schwarz N, Jalbert M, Noah T, Zhang L (2021) Metacognitive experiences as information: Processing fluency in consumer judgment and decision making. *Con. Psy. Rev.* 4(1):4-25.

Seo BG, Park DH (2019) The effect of message framing on security behavior in online services: Focusing on the shift of time orientation via psychological ownership. *Comput. Hum. Behav.* 93:357-369.

Seo K, Dillard J (2019) The Persuasive Effects of Two Stylistic Elements Framing and Imagery. *Commun. Res.* 46(7):891-907.

Septiari D (2020) Impact of Warning Messages on the Reliance Level on Decision Aids under the Framing Effect. *Asian J. Bus. Account.* 13(1).

Silva RR, Chrobot N, Newman E, Schwarz N, Topolinski S (2017) Make it short and easy: Username complexity determines trustworthiness above and beyond objective reputation.

Front. Psychol. 8:2200.

Smith HJ, Dinev T, Xu H (2011) Information Privacy Research: An Interdisciplinary Review. *MIS Q.* 35(4):989-1015.

Takemura K (1994) Influence of Elaboration on the Framing of Decision. *J. Psych.* 128(1):33-39.

Tsai JY, Egelman S, Cranor L, Acquisti A (2011) The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study. *Inf. Systems Research* 22(2):254-268.

Williams M, Nurse JR, Creese S (2016) Privacy salience: Taxonomies and research opportunities. Lehmann A, Whitehouse D, Fischer-Hubner S, Fritsch L, Raab C, eds. *Proc. 11th IFIP Intl Summer School on Privacy and Identity Management* (Springer, Sweden), 263-278.

Winkielman P, Huber DE, Kavanagh L, Schwarz N (2012) Fluency of consistency: When thoughts fit nicely and flow smoothly. Gawronski B, Strack F, eds. *Cognitive consistency: A fundamental principle in social cognition* (Guilford Press, New York), 89-111.

Xiao B, Benbasat I (2015) Designing warning messages for detecting biased online product recommendations: An empirical investigation. *Inf. Syst. Res.* 26(4):793-811.

Xu L, Duan JA, Whinston A (2014) Path to purchase: A mutually exciting point process model for online advertising and conversion. *Manage. Sci.* 60(6):1392-1412.