Journal of Global Information Management
Volume 30 • Issue 1

Better Not Let Me Know:
Consumer Response to Reported Misuse of Personal Data in Privacy Regulation

Chenwei Li, Xi'an Jiaotong-Liverpool University, China
Jie Chu, Xi'an Jiaotong-Liverpool University, China
https://orcid.org/0000-0001-7857-4176
Leven J. Zheng, Hong Kong Metropolitan University, Hong Kong*

ABSTRACT

Customers' concerns about inappropriate use of personal information can create potential threats that jeopardize the proliferation of emerging markets. This study aims at investigating how the adaptive and maladaptive responses of consumers are driven by perceived threat and perceived efficacy of external cues theoretically and how consumers react to the reported misuse of personal data in privacy regulation in the emerging online market. Online experiments were conducted to test the research model. This study contributes to the extension of extended parallel process model by theoretically examining the relationships between perceived threat and perceived efficacy and offers insights into the improvement of privacy regulation from the consumer perspective.

KEYWORDS

Adaptive and Maladaptive Response, Customers, Extended Parallel Process Model, Privacy Regulation

INTRODUCTION

Privacy issues have become increasingly important with the rapid adoption of digital technologies; in general, people have become increasingly worried about their online privacy (Acquisti et al., 2015; Gerber et al., 2018; Ginosar & Ariel, 2017; Preibusch et al., 2016). As people's lives are being embedded in various digital platforms, personal data are easily recorded, monitored, and shared without consent (Wu et al., 2019). While the collection and use of personal data can provide advantages to individuals and businesses (Sánchez & Viejo, 2017), it also encourages the abuse of consumers' personal data and may cause serious changes to their behavior (Hong et al., 2019). Consumer concerns regarding the inappropriate use of personal data can also create potential threats, jeopardizing participation in the online market. Therefore, it is imperative for both academia and industry to understand privacy concerns and develop effective strategies to protect consumer privacy.

Privacy regulation is an instrument of institutional privacy protection that provides a sense of security and safety (Nam, 2019). It is applied widely, across various areas (Banerjee et al., 2018). Lwin et al. (2007) argue that regulation is important for decreasing privacy concerns so that users will be less worried about the abuse of their personal data if companies behave responsibly and implement all necessary protection rules. Similarly, Ginosar and Ariel (2017) state that privacy

DOI: 10.4018/JGIM.306246 *Corresponding Author

concerns could be significantly decreased if sufficient resources were provided. Notably, most prior studies focus on emphasizing the benefits of offering more consumer control in privacy regulations, while overwhelmingly ignoring the potential negative effects of too much control.

According to Westin (1967), information privacy is defined as "the ability of the individual to control the terms under which personal information is acquired and used." From this definition, it may be interpreted that one way to decrease the level of perceived privacy risk for consumers is to increase their control over personal information. Therefore, strengthening privacy protection through offering more control has been a central theme of recent regulations. There are several ways through which regulations can strengthen consumer control over personal data. For instance, previous regulations usually attached importance to notice that no data should be collected from individuals who were not aware it was being collected (Langenderfer & Cook, 2004). Another important method is to ensure that consumers are informed about the misuse of their personal data and can react promptly. For example, globally, many privacy regulations share common principles. These include prompt reporting to users if their personal data are being sold to or shared with a third party.

Although increasing control is well intentioned, enhancing it unilaterally may restrict consumer rights and harm them emotionally (e.g., regarding the choice of not being informed about the misuse). When facing restrictions in regard to accessible alternative options, people may perceive themselves as having limited freedom of choice and will thus be motivated to restore this freedom (Rosenberg & Siegel, 2018). This motivational state may lead to undesired coping responses, such as negative attitudes and emotions (Chang & Wong, 2018). Therefore, the reported misuse of personal data could lead to undesired coping consequences.

Most studies of privacy focus on desired coping responses that are adaptive, such as avoiding IT threats (Liang & Xue, 2009, 2010) and adopting protective behavior (Boss et al., 2015; Johnston et al., 2015; Johnston & Warkentin, 2010). For example, Xu et al. (2009) found that government regulation is negatively related to the perceived risk of personal information disclosure. Miltgen and Smith (2015) determined that higher levels of perceived privacy regulatory protection were associated with higher levels of trust and lower levels of privacy concerns. Andrew and Baker (2019) argued that privacy regulations could have a significant influence on protecting individual privacy. However, very little research has been conducted to investigate consumers' undesired or maladaptive reactions toward the reported misuse of personal data.

The extended parallel process model, as an expansion of previous fear-oriented theories, adds a secondary appraisal process in which individuals' assessments of perceived threat and efficacy determine whether they will engage in a danger control process or a fear control process with corresponding adaptive or maladaptive responses (Witte, 1992). It offers a framework to study the parallel responses of consumers, such as a recognition or denial response (Leventhal, 1970). In the context of technology-based threats, adaptive responses refer to the safeguarding measures undertaken when users perceive a threat, driven by human nature; conversely, maladaptive responses refer to the passive avoidance of a threat (Liang & Xue, 2009). However, it is important to note that the extended parallel process model does not specify what conditions lead to recognition or a denial response, nor how these two responses are evoked by external cues (De Hoog et al., 2007). Although the perceived threat and efficacy of external cues are considered important (Popova, 2012; Ruiter et al., 2014; Witte, 1994), to the best of the authors' knowledge, no research has examined the role of threat- and efficacy-related perceptions based on the extended parallel process model. Therefore, this study tests the relationship between perceived threat and perceived efficacy within the extended parallel process model.

Recent developments in business management and information systems have led to fierce debate regarding how to protect consumer privacy and how much control should be given in the online environment (Ginosar & Ariel, 2017; Liu & Du, 2020; Lonkani et al., 2020; Rahman et al., 2020; Sánchez & Viejo, 2017; Sengupta, 2020). This is particularly the case with emerging online markets, which are often confronted with a mismatch between privacy regulation and its practical

implementation (Budak et al., 2015). To match available service providers and consumers with their respective needs, most online platforms try to collect as much personal information as possible, including names, dominant language, email addresses, country, mobile phone number, password, and credit card numbers. This mechanism ensures that privacy issues are more salient for online consumers and more meaningfully examined. Accordingly, in this study, the following research questions are proposed:

Research Question 1 (RQ1): How are the adaptive and maladaptive responses of consumers driven by the perceived threat and perceived efficacy of external cues?

Research Question 2 (RQ2): How do consumers react to the reported misuse of personal data in privacy regulations in the emerging online market?

To address these two questions, this study develops a research model drawing on the extended parallel process model to examine the influence of reported misuse of personal data on consumer responses, both adaptive and maladaptive. Online experiments are employed to test the research model. Specifically, this study varies the types of reported personal data misuse according to general privacy regulation principles. The focus is on the treatment of different types of reported data misuse and consumer responses to these. The subjects were not informed of the experiment's purpose; as a result, their responses should reflect objective perceptions.

This study contributes to the existing literature in several respects. First, differing from prior regulations that emphasize desired coping responses that are adaptive, it takes into account the psychology of consumer information processing in decision-making, and capture both adaptive and maladaptive responses to the reported misuse of personal data. In this way, not only are consumer bilateral responses tested, but also the two approaches through which the responses are activated (i.e., danger control process and fear control process) are explored. Second, building upon the extended process model framework, an empirical analysis is performed to investigate how consumers' adaptive and maladaptive responses are driven by perceived threat and efficacy. Based on the results, and although the proposed moderation effect of the perceived threat has not been confirmed, it seems that response efficacy and self-efficacy lead to adaptive and maladaptive responses, respectively. This is achieved through the activation of protection and defensive motivations. Third, this study examines how consumers might react to the reported misuse of personal data in privacy regulations, in the context of the emerging online market. Our empirical results suggest that certain types of misuse should be reported preferentially over others, which could be useful for a regulatory body when choosing a data privacy regime. Finally, the results of this study provide several practical insights into information privacy issues from consumer perspective.

The remainder of this paper is organized as follows. In the next section, a retrospective overview of prior privacy regulations is presented. This is followed by a section that reviews the academic research on privacy. Then, the theoretical foundation is discussed. In the subsequent section, the research model is developed and hypotheses proposed. Next, a description of the methodology employed is provided. The main findings are presented next, followed by a section that discusses practical implications (based on the results). In the last section, the limitations and future research directions are discussed.

PRIVACY REGULATIONS

Given the importance of privacy, one strategy when dealing with privacy issues is regulation (Chellappa & Shivendu, 2007). Globally, several regulations are already in the spotlight. For example, the Personal Information Protection and Electronic Documents Act, the enforcing federal privacy law in Canada since April 2000, provides clear ground rules for private-sector organizations regarding how to handle personal information collected during commercial activities. The act requires organizations

to collect, use, or disclose personal information subject to an individual's right to privacy. Under this act, individuals have the right to access their personal information and challenge the information's accuracy. The Fair Information Practice Principles, which have been accepted as the guiding standards for industry information regulation in many jurisdictions in the United States (Langenderfer & Cook, 2004), also address the collection and use of personal data. These principles provide a framework to protect privacy through reducing the information asymmetry between information owners and collectors, and through enhancing an information owner's perceived control in the process of information circulation. Similar regulations, such as the General Data Protection Regulation, the California Consumer Privacy Act, and the Chinese Cybersecurity Law have been enacted more recently, with the aim of enhancing personal data protection.

These privacy regulations share some common principles. For example, involved users must be able to request information about why their personal data are being collected; users must be informed if their personal data will be sold or shared with a third party; users must have access to their data, be able to download it, and be able to request that their data are deleted. Along with the development of needs, regulations emphasize giving consumers adequate control over the processing of their data. While enhanced information regulations could help to maintain privacy and security regarding consumers' personal information, the associated business compliance costs may be passed along to consumers, or businesses may find it difficult to gain current profitability owing to the personal information-related law, and will choose to stop providing consumers relevant services. Thus, it might be consumers who will pay for enhanced rights around privacy. It is not a question of whether consumers value privacy, but whether enhanced privacy regulations are good value. Therefore, it is imperative, in practical terms, to consider the psychology of how consumers process information in decision-making (Van Ooijen & Vrabec, 2019). By evaluating privacy regulations through a psychological behavior lens, it is possible to predict the effectiveness of enhanced privacy regulations, in terms of consumers' actual responses (Van Ooijen & Vrabec, 2019). This also helps solve a long-standing question regarding how a regulatory body should choose a regime that protects consumer privacy while not limiting the growth of a new economy (Chellappa & Shivendu, 2007). In this study, the authors will examine the effect of reported personal data misuse on consumer responses.

LITERATURE REVIEW

Since Chellappa and Shivend (2007), academic debate has emerged on the formulation of ideal legal frameworks calling for effective regulations that consider both technological and behavioral rationales behind the protection of consumer personal data. The results indicate that robust business policies and governmental regulations could reduce privacy concerns. More interestingly, the results also show that a lack of governmental regulation can result in consumers attempting to regain balance in matters of control. Contributing to the discussion about whether and how privacy regulations have struck a balance between data-related privacy and surveillance concerns, Andrew and Baker (2019) argue that privacy regulations may have a significant influence on protecting individual privacy. Adjerid et al. (2016) have also noted the importance of a balance between overregulation and the healthy growth of changes to how information is handled. How to deal with privacy issues without overregulating information disclosure is an issue that must be addressed by research.

However, many privacy-related studies (Miltgen & Smith, 2015; Xu et al., 2009, 2012) show that it is important to consider an individual's decision-making in regulation research. Van Ooijen and Vrabec (2019) highlight that, although the General Data Protection Regulation takes important steps in addressing threats to individual control from a behavioral perspective, some pitfalls in human decision-making remain that must be considered further in the development of these regulations. Anic et al. (2019) link government regulation with privacy concerns and examine consumer responses to privacy threats. Their results show that respondents would like to acquire more control over their personal data, and that government regulation is perceived as weak when protecting their privacy.

Consumer perceptions or preferences can influence their behavior significantly. The importance of behavioral perspectives on decision-making has been recognized and accepted gradually (Adjerid et al. 2018). Thus, in this study, the authors adopt a behavioral perspective to investigate consumer coping responses to privacy regulations.

Although it is undertaken with the positive intention of alleviating consumer privacy concerns, enhancing control unilaterally may restrict consumer rights and harm them emotionally (e.g., regarding the choice to not be informed about misuse). When facing restrictions on the accessibility of alternative options, people may perceive themselves as having limited freedom to choose, and thus are often motivated to restore their freedom when facing threats (Rosenberg & Siegel, 2018). A motivational state that prompts a person to act against the source of a threat and redeem their freedom is defined as psychological reactance (Brehm & Brehm, 1981). This can result in undesired coping responses, such as negative attitudes and emotions (Chang & Wong, 2018). Individuals will experience reactance to the extent to which perceived freedoms are limited (Brehm & Brehm, 2013). Therefore, the reported misuse of personal data could possibly lead to undesired coping consequences.

Notably, most studies on privacy focus on desired coping responses that are adaptive, such as the avoidance of IT threats (Liang & Xue, 2009, 2010) and the adoption of protective behavior (Boss et al., 2015; Johnston et al., 2015; Johnston & Warkentin, 2010). However, relatively little research has been conducted on consumer maladaptive reactions to privacy regulations. Because adaptive and maladaptive responses co-exist in individuals who are coping with demanding events (Endler & Parker, 1990; Witte & Allen, 2000), both types of responses must be considered to understand how people deal with privacy threats. As new privacy regulations come into force, collaborative work with all stakeholders is needed to develop a coherent privacy framework that incorporates compatible approaches about privacy protection. Thus, this study examines the effect of the reported misuse of personal data on consumer adaptive and maladaptive responses, while also considering consumer psychology. Adaptive responses are defined as safeguarding measures when users perceive an IT threat, while maladaptive responses refer to the passive avoidance of a threat (Liang & Xue, 2009). In this study, the authors adopt these definitions and apply them in the context of emerging online markets through the observation of permissions enaction.

THEORETICAL FOUNDATION

To study consumer responses to enhanced privacy regulations, the authors draw on the extended parallel process model (Popova, 2012; Witte & Allen, 2000) to formulate the theoretical model.

The extended parallel process model is an expansion of previous fear-oriented theories that considers a secondary appraisal process in which an individual's assessment of perceived threat and perceived efficacy determine that person's engagement in the danger control or fear control process, as well as the corresponding adaptive and maladaptive responses (Witte, 1992). Specifically, people tend to engage in a fear control process if there is high perceived threat but low perceived efficacy, believing that they are unable to deter the threat. Thus, it is highly likely that they engage in maladaptive responses. In contrast, people tend to engage in a danger control process if there is high perceived threat and perceived efficacy, because they are confident deterring the threat, and thus take adaptive actions (Witte, 1994). Key constructs in the extended parallel process model are described below.

Perceived Threat

A threat is considered an existing danger in the environment. Perceived threat is a key variable of the persuasive processes in the fear appeal research, which comprises two dimensions: perceived severity of the threat and perceived susceptibility to the threat (Popova, 2012; Witte & Allen, 2000). The first dimension refers to an individual's beliefs about the significance or magnitude of the threat, while the second dimension refers to individual's beliefs regarding their risk of experiencing the threat. It is important to note that the perceived fear appeal not only induces cognitions that a threat exists but

also conveys the severity of the threat and the target's susceptibility to the threat (Rogers & Deckner, 1975; Witte, 1992). That is, an individual will establish beliefs, such as the seriousness of a threat and the probability of experiencing that threat, under the awareness of being threatened.

Perceived Efficacy

An efficacy points to the "effectiveness, feasibility, and ease with which a recommended response alleviates or helps in avoiding a threat" (Popova, 2012). According to Popova (2012), there are two forms of perceived efficacy: response efficacy and self-efficacy. The former corresponds to the cognitions of the effectiveness of the recommended response in averting the threat, and the latter refers to an individual's ability to perform the recommended response to deal with the threat.

Danger Control Process

The danger control process is a primarily cognitive process where individuals evaluate a situation and develop corresponding countermeasures (Witte, 1992, 1994). In the danger control process, the risk is perceived as significant and individuals perceive that their ability to deter the threat is strong. In other words, individuals believe that they are able to effectively take protective measures to remove the risk. This leads to a typical adaptive response.

Fear Control Process

The fear control process is more emotional and may occur beyond conscious awareness, especially when individuals are faced with a significant threat (Witte, 1992, 1994). In the fear control process, the risk is perceived as severe and unavoidable. Individuals believe that they are unable to perform any recommended response; thus, a subconscious defense process will be activated to escape from reality. This leads to a typical maladaptive response.

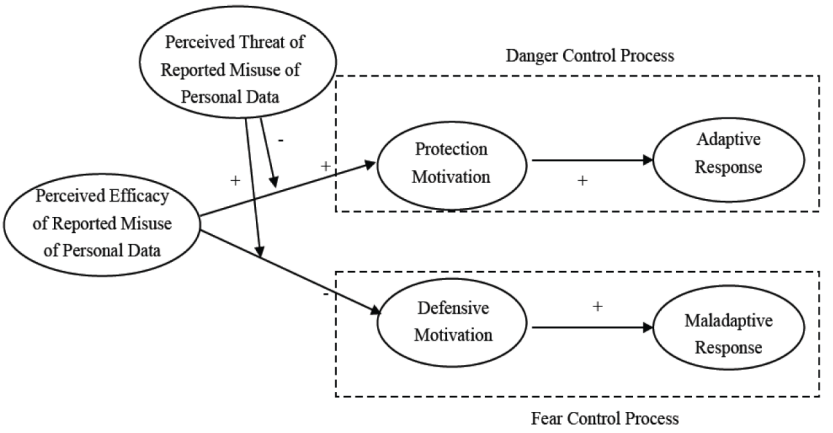
In general, with the assumption that threats are cognitively evaluated, two parallel processes typically result from the extended parallel process model: the fear and the danger control processes (De Hoog et al., 2007). A perceived threat contributes to the extent of a response, whereas perceived efficacy contributes to the nature of the response (Witte, 1994). Fear control initiates responses such as denial or avoidance, which can reduce unpleasant feelings. Danger control copes with the danger and directly lessens its effect (De Hoog et al., 2007; Leventhal, 1970).

It is critical to note that the relationship between a perceived threat and perceived efficacy is characterized by its multiplicative manner. However, the extended parallel process model does not specify the conditions under which the fear control process or the danger control process emerge, how they interact, or how individuals alternate between the two processes (De Hoog et al., 2007). To the authors' knowledge, the interactive effects of the perceived threat and perceived efficacy have not been explored in the literature; thus, a theoretical rationale to support the possible assumptions is required. The multiplicative relationship between a perceived threat and perceived efficacy, as suggested by Witte (1994), has rarely been addressed (Popova, 2012; Witte & Allen, 2000). Although some scholars advocate that efficacy is typically more important than threat (Popova, 2012; Ruiter et al., 2014), the authors of the present study believe that some effort is still required to further investigate the relationship between different modes of coping.

Research Model and Hypotheses

To test the underlying relationship between perceived efficacy and perceived threat while capturing both consumer adaptive and maladaptive responses toward the reported misuse of personal data, a research model is proposed based on the extended parallel process model (see Figure 1). Because perceived efficacy contributes to the nature of the response while perceived threat contributes to the extent of a response (Witte, 1994), it is speculated that a moderation relationship may exist between them.

Figure 1. Conceptual research model



Perceived Efficacy and Protection/Defensive Motivation

The response efficacy dimension of perceived efficacy evaluates how effectively an adaptive response copes with a threat. Response efficacy may increase an individual's active coping responses, as that person knows how to detect and reduce potential risks (Wang et al., 2017). Response efficacy increases the likelihood that someone will engage in adaptive motivation. This is because individuals with a high response efficacy are more confident that, when faced with external threats, the protective actions they undertake will be effective. The self-efficacy dimension of perceived efficacy is the expectancy of an individual's capability to perform a recommend response that significantly influences their intention to take action in various contexts. Self-efficacy may give people confidence to handle risky situations and deal with threats. Thus, instead of engaging in worry or avoidance, it increases the likelihood of engaging in defensive motivation (Wang et al., 2017). As mentioned above, when using online services, an individual's perception of high response efficacy when responding to risks aroused by the reported misuse of personal data drives a high protection motivation through the danger control process. By contrast, a perception of high self-efficacy may decrease an individual's concern and belief in their capability to handle risks and thus drive a defensive motivation through the fear control process. Therefore, the following hypotheses are proposed:

Hypothesis 1 (H1): Consumers' perceived response efficacy increases their protection motivation in the reported misuse of personal data.

Hypothesis 2 (H2): Consumers' perceived self-efficacy increases their defensive motivation in the reported misuse of personal data.

Perceived Threat and Perceived Efficacy

As suggested by the extended parallel process model, the threat and coping appraisal is an ordered process: threat appraisal takes place first and leads to coping appraisal. A perceived threat contributes to the extent of a response, whereas perceived efficacy contributes to the nature of the response (Witte, 1994). If people perceive a potential threat, they will use the coping appraisal to find an appropriate countermeasure. If a potential threat is not perceived or is too low, there will be no further processing of the threat owing to its irrelevance. Certainly, in this situation a person will not initiate any coping strategies. When people believe that a more serious consequence will be caused by a threat (i.e., an increase in perceived severity), their defensive motivation, as aroused by self-efficacy, will decrease

because of a loss of faith in their ability to adequately cope with the threat. When people believe that there is a much higher chance of being affected by the threat (an increase in the perceived susceptibility), their protection motivation, as aroused by response efficacy, will be increased because it considers the danger as being significant and generates a feeling that privacy is at risk; thus, action must be taken to deal with the threat. When a perceived threat is detected, it induces motivation to cope with that threat (Boss et al., 2015; Johnston et al., 2015). When a perceived threat arouses the fearful feeling of privacy being at risk, a defensive motivation is more likely to be activated through emotional adjustment (Popova, 2012); otherwise, protection motivation is more likely to be activated if a danger is successfully detected. Therefore, the following hypotheses are proposed:

Hypothesis 3 (H3): Consumers' perceived susceptibility of external cues positively moderates the relationship between response efficacy and their protection motivation in the reported misuse of personal data.

Hypothesis 4 (H4): Consumers' perceived severity of external cues negatively moderates the relationship between self-efficacy and their defensive motivation in the reported misuse of personal data.

Protection/Defensive Motivation and Behavior Response

When analyzing consumer responses, it is important to consider the available behavior in the context of emerging online markets. Usually, two features appear relevant to user privacy: application (app) permissions and real-time location disabling, especially when using service apps on smartphones. To provide the online services, companies or platforms often access consumers' personal data. While this access is legitimate, details are commonly traded with third parties (Schneier, 2015). Fortunately, privacy permissions can restrict access on smartphones. When applications are not allowed to "read" personal details, they cannot share them with third parties. Therefore, in this study, the authors observe how consumers will react through permissions if data are shared with others. Real-time location use can support functions such as navigation and fitness tracking through the location of a device being monitored (Dogruel et al., 2017). When an individual wants to limit this function, they can disable their real-time location. This function can then be briefly re-enabled when required. Therefore, the authors observe how consumers react through real-time location disabling if the position of a smartphone is monitored. It is worth noting that two app permissions are generally concerned with private data: contact lists (associated with phone numbers) and account information (e.g., including a head portrait, nickname, district and gender).

In the literature, adaptive responses are defined as safeguarding measures when users perceive an IT threat, which accepts responsibility by taking remedial actions; maladaptive responses are referred to the passive avoidance of the threat. Returning to the research model, with a protection motivation, people believe that a desired response will be effective (i.e., response efficacy) and that they will be able to perform the action (i.e., self-efficacy). Here, the costs of performing the action will not exceed the perceived benefits (i.e., response costs). Thus, an adaptive response will be obtained. For instance, when people believe their privacy is exposed to risk, they will take protective action by denying app permissions and disabling real-time location functions, believing that they are able to deal with the risks. With a defensive motivation, people think that a threat is fearful (i.e., perceived severity), so that they may be injured or attacked (i.e., perceived vulnerability), and the costs of performing the action will exceed the perceived benefits (i.e., response costs). Thus, a maladaptive response will be obtained, such as allowing app permissions and enabling real-time location functions, focusing on the denial of a possible crisis. Therefore, the following hypotheses are proposed:

Hypothesis 5 (H5): Consumers' protection motivation will lead to their adaptive responses, such as deny app permissions and disable real-time location.

Hypothesis 6 (H6): Consumers' defensive motivation will lead to their maladaptive responses, such as allow app permissions and enable real-time location.

METHODOLOGY

An online experiment was adopted to study the influence of the reported misuse of personal data on consumer responses. Participants qualified for the study if they had experience in using online service apps. As compensation, participants received a reward after they completed the experiment.

Consumers of the following four apps were recruited as targeted participants: (a) a car sharing app named DiDi; (b) a food delivery app named Meituanwaimai; (c) a home sharing app named Airbnb; and (d) an e-healthcare app named Haodaifu. All these online service apps may pose some privacy risks as they share location-based information (DiDi and Meituanwaimai) or personal- and health-related information (Airbnb and Haodaifu), which makes privacy-related decision-making salient and meaningful for this study.

Data Collection

The online experiment was presented via a web- and mobile-based survey with anonymity assured. Over a 4-week period, undergraduate and graduate students from two universities (one in the north and the other in the south to ensure the generalizability of samples) in mainland China were invited to answer the questionnaire. Although the use of student samples has been challenged previously, it has been recognized and accepted in recent years (Hui et al. 2007). Meanwhile, as real users of online service apps, their answers are representative and should not be of concern.

Among 332 complete answers, 102 participants received various messages about the reported misuse of personal data with valid manipulation, while 106 participants received no message of any kind. Answers from 124 participants were removed from the data set either owing to invalid manipulation (here, invalid manipulation means that the respondents chose to skip the message and thus the message was not read) or an invalid answer (invalid answers means that the respondents failed to pass the attention check or spent far more time in answering questions than a reasonable threshold). The respondents were roughly evenly divided by gender (55.1% vs. 44.9%) and most were in the age group of 18 to 45. Demographics are reported in Table 1. Data for control variables were also collected, and include respondents' gender, age, education, income level, and prior internet experience.

Table 1. Respondent demographics

Demographic Variables		Frequency and percentage (N = 332)	
Gender	Male	183	55.1%
	Female	149	44.9%
Age	< 18	2	0.6%
	18–25	263	79.2%
	26–35	34	10.2%
	36–45	21	6.3%
	46–55	9	2.7%
	> 55	3	0.9%

Table 1 continued on next page

Table 1 continued

Demographic Variables		Frequency and percentage (N = 332)	
Educational level	Below & high school	4	1.2%
	Bachelors	294	88.6%
	Masters	19	5.7%
	Doctors	15	4.5%
	Others	0	0%
Monthly income	None	201	60.5%
	< 1500RMB	21	6.3%
	1501–3000RMB	24	7.2%
	3001–5000RMB	19	5.7%
	5001–8000RMB	22	6.6%
	8001–10000RMB	15	4.5%
	> 100000RMB	30	9.0%
Frequency	< 1 time per month	172	51.8%
	2–3 times per month	90	27.1%
	1–3 times per week	31	9.3%
	4–6 times per week	7	2.1%
	> 1 time per day	1	0.3%
Duration	< 1 month	27	8.1%
	1 to < 3 months	27	8.1%
	3 to < 6 months	32	9.6%
	6 to < 12 months	39	11.7%
	Above 1 year	197	59.3%

Experimental Design and Procedure

The study was designed as an online survey–based experiment, displaying different types of the reported misuse of personal data. To address the research questions, a two (reported collected data vs. non-reported collected data) × two (reported sold data vs. non-reported sold data) experiment was conducted, with four scenarios manipulating the two types of reported misuse of personal information (data collected by a service company and data sold to other third parties). Participants were randomly assigned to either one of the four experimental groups. Table 2 overviews the four experimental groups.

Table 2. Overview of experimental groups

Categorization	Reported sold data	Non-reported sold data
Reported collected data	Experimental group #1	Experimental group #2
Non-reported collected data	Experimental group #3	Experimental group #4

For the manipulation of the reported misuse of personal data, a page in the online survey contained a message about the use of consumers' personal data. The participants were given a description of the misuse of their personal data (either data collected by the platform, or data sold to other third parties after using the app, according to their randomly assigned experimental group). They were asked to indicate their choice after reading by pressing either the "OK, I have read the message carefully and been informed" button (indicating acceptance of the message and the success of manipulation), or the "Please skip this message because I am not interested in it" (indicating that they did not read the message, and the failure of manipulation).

Participants in the four experimental conditions were randomly assigned into different groups. For Group #1, the message showed that users' personal data were both sold to third parties and were collected by the service company. In Group #2, the content of the message revealed that users' personal data were collected by the service company but no data were sold to third parties. In Group #3, the content of the message showed that users' personal data were sold to third parties but did not mention anything about data collection. In Group #4, there was no reported misuse of personal data, and was used as a baseline for the response valuation. The pretended app evaluation tasks took place after the manipulation. Participants' privacy attitudes and perceptions were monitored immediately after the evaluation tasks. Their responses in terms of allowing/denying app permissions and enabling/disabling real-time locations were captured, as well as demographic factors.

It is important to note that deception was used to increase realism of the experiment results. For implementation of the experiment, participants were informed that the experiment's goal was to understand and refine the design of apps they had used previously. A brief introduction to the pretended purpose was provided at the beginning of the questionnaire. Participants were given several tasks to complete, requiring them to recall their past use experience and answer the questions. After completing the evaluation tasks, participants were asked to answer another set of questions, which addressed this study's real concern.

To increase external validity, the authors opted for a field setting that allowed participants to use the devices as in their daily life. An instructional manipulation check within the questions was also included in the questionnaire. In one of the questions, participants were asked to indicate their attentiveness by replying "Strongly Disagree," which did not serve any other purpose but could check their level of concentration (Oppenheimer et al. 2009).

Manipulation Check

To ensure that respondents were successfully manipulated by the misuse-reporting message, they were asked to indicate whether they had read the message completely by ticking the corresponding button. To assess the effectiveness of message treatment in manipulation, a multivariate analysis of variance (MANOVA) using STATA was conducted through the comparison of perceived severity, perceived susceptibility, response efficacy and self-efficacy between pre- and post-response data (see Table 3). These findings indicated that, when exposed to the misuse-reporting message, previous perceptions of perceived severity and self-efficacy decreased significantly, but the changes in perceived susceptibility and response efficacy were not significant. The results confirm that the message treatment could support the internal validity of the experimental design.

Table 3. Results of manipulation effectiveness

Variable	Pre-test mean	Post-test mean	*F*-test	Significance
Perceived severity	$M = 6.35$ ($SD = 1.28$)	$M = 5.80$ ($SD = 1.48$)	8.14	$p < 0.01$
Perceived susceptibility	$M = 5.78$ ($SD = 1.41$)	$M = 5.49$ ($SD = 1.50$)	2.11	Not significant
Response efficacy	$M = 4.78$ ($SD = 1.33$)	$M = 4.69$ ($SD = 1.50$)	0.18	Not significant
Self-efficacy	$M = 3.75$ ($SD = 1.28$)	$M = 3.22$ ($SD = 1.49$)	7.67	$p < 0.01$

Questionnaire Items

The constructs were operationalized using previously validated item measures. Items were adapted from prior studies in privacy research (see Table 4). Perceived severity of threat, perceived susceptibility of threat, self-efficacy, and response efficacy were measured using items adopted from Johnston et al. (2015), which have also been used across many studies. Protection motivation, defensive motivation, adaptive response and maladaptive response were derived from Liang and Xue (2010) and Popova (2012), both specialized in this research context.

Table 4. Measurement Items for principal constructs

Item	Description	Source
Perceived severity (perceived threat)	1. If my personal data has been collected by the online platform or company/sold to third parties, the consequences would be severe (TSEV1). 2. If my personal data has been collected by the online platform or company/sold to third parties, the consequences would be serious (TSEV2). 3. If my personal data has been collected by the online platform or company/sold to third parties, the consequences would be significant (TSEV3).	Adapted from Johnston et al. (2015)
Perceived susceptibility (perceived threat)	1. My personal data reported to be collected/sold is at risk of being abused (TSUS1). 2. It is likely that my personal data, reported to be collected/sold, will be abused (TSUS2). 3. It is possible that my personal data, reported to be collected/sold, will be abused (TSUS3).	Adapted from Johnston et al. (2015)
Self-efficacy (perceived efficacy)	1. Protecting my personal data reported to be collected/sold from abuse is easy to do (SEFF1). 2. Protecting my personal data reported to be collected/sold from abuse is convenient to do (SEFF2). 3. I am able to protect my personal data reported to be collected/sold from abuse without much effort (SEFF3).	Adapted from Johnston et al. (2015)
Response efficacy (perceived efficacy)	1. The protective measure will take/taken by me to protect my personal data reported to be collected/sold works (RESP1). 2. The protective measure taken by me to protect my personal data reported to be collected/sold is effective (RESP2). 3. If I take action, my personal data reported to be collected/sold is more likely to be protected (RESP3).	Adapted from Johnston et al. (2015)

Table 4 continued on next page

Table 4 continued

Item	Description	Source
Protection motivation	1. I intend to protect my personal data reported to be collected/sold from abuse (PM1). 2. I predict I will protect my personal data reported to be collected/sold from abuse (PM2). 3. I plan to protect my personal data reported to be collected/sold from abuse (PM3).	Adapted from Liang and Xue (2010)
Defensive motivation	1. When reading the reported collection/sell of my personal data, I spend additional time thinking about it (DM1). 2. I think that the reported collection/sell of my personal data is exaggerated (DM2). 3. I think that the reported collection/sell of my personal data is distorted (DM3).	Developed from Liang and Xue (2010) and Popova (2012)
Adaptive response	1. I deny contacts list permissions while using online services on my smartphones (AR1). 2. I deny account information permissions while using online services on my smartphones (AR2). 3. I disable real-time location while using online services on my smartphones (AR3).	Developed from Liang and Xue (2010) and specific research context
Maladaptive response	1. I allow contacts list permissions while using online services on my smartphones (MR1). 2. I allow account information permissions while using online services on my smartphones (MR2). 3. I enable real-time location while using online services on my smartphones (MR3).	Developed from Liang and Xue (2010) specific research context

Results Analysis

This section begins with an assessment of the measurement model and the structural model. Following that, a manipulation check and discussion are undertaken. The measurement model and structural model are assessed based on data from the untreated group to answer the first research question, through conducting a partial least squares analysis using SmartPLS3. The manipulation check and discussion were conducted to answer the second research question.

Measurement Model Assessment

The internal consistency reliabilities of constructs were evaluated via composite reliability scores, which were satisfactory (see Table 5).

Table 5. Measurement statistics of constructs

Construct	Factor loadings	Composite reliability	Cronbach's alpha	AVE
Perceived severity	0.867	0.949	0.920	0.861
	0.948			
	0.966			
Perceived susceptibility	0.932	0.966	0.947	0.905
	0.975			
	0.947			
Self-efficacy	0.913	0.935	0.910	0.827
	0.930			
	0.884			
Response efficacy	0.964	0.976	0.962	0.930
	0.974			
	0.956			
Protection motivation	0.903	0.943	0.909	0.846
	0.921			
	0.936			
Defensive motivation	0.963	0.961	0.919	0.925
	0.961			
Adaptive response	0.817	0.849	0.734	0.652
	0.834			
	0.770			
Maladaptive response	0.942	0.920	0.829	0.852
	0.904			

From Table 5, all constructs exhibited sufficiently high reliability with Cronbach's Alpha above the recommended 0.70 threshold. Convergent validity was assessed based on outer loadings and average variances extracted (AVEs). Loadings of all retained indicators on their related theoretical constructs were significant ($p < 0.01$) and exceeded the recommended 0.70 threshold in the measurement model. All AVEs were greater than 0.50 and higher than the highest shared variance between all possible pairs of constructs for each construct.

Table 6. Heterotrait–monotrait ratio of constructs

Construct	TSEV	TSUS	SEFF	RESP	PM	DM	AR	MR
Perceived severity (TSEV)		0.574	0.225	0.390	0.408	0.276	0.335	0.147
Perceived susceptibility (TSUS)			0.249	0.239	0.471	0.250	0.530	0.048
Self-efficacy (SEFF)				0.584	0.360	0.662	0.395	0.357

Table 6 continued on next page

Table 6 continued

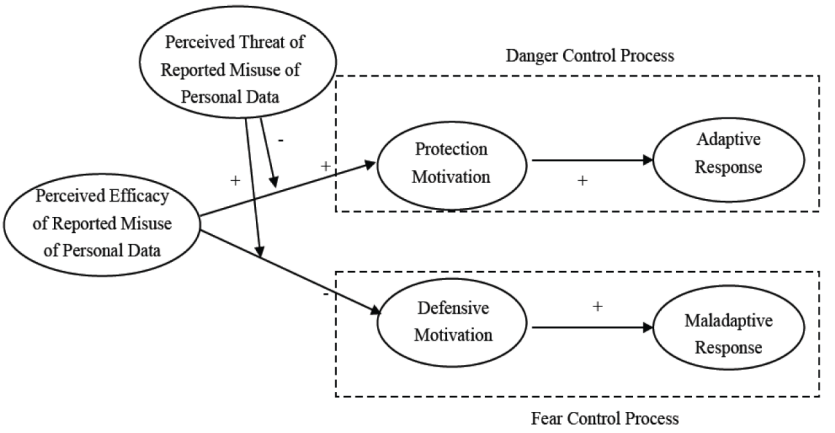
Construct	TSEV	TSUS	SEFF	RESP	PM	DM	AR	MR
Response efficacy (RESP)					0.471	0.473	0.292	0.267
Protection motivation (PM)						0.415	0.465	0.214
Defensive motivation (DM)							0.338	0.559
Adaptive response (AR)								0.351
Maladaptive response (MR)								

Discriminant validity was assessed via cross-loading analysis and the heterotrait–monotrait (HTMT) ratio of correlations (Henseler et al. 2015). Outer loadings of items on the certain construct should exceed the cross-loadings on other constructs. It can be seen from the factor loadings (see Table 8 in the Appendix) that satisfactory discriminant validity was obtained in the model. In addition, the HTMT ratio should be below 0.85 to declare discriminant validity conceptually (Henseler et al. 2015), and this was met in the model (see Table 6).

Structural Model Assessment

Figure 2 displays the path coefficients. The results indicate that consumer response efficacy had a positive relationship with protection motivation ($\beta = 0.327$, $t = 3.278$, $p < 0.001$), and that self-efficacy had a positive relationship with defensive motivation ($\beta = 0.524$, $t = 6.723$, $p < 0.001$). This supports H1 and H2. The results were also highly significant for the effect of protection motivation on adaptive response ($\beta = 0.386$, $t = 3.616$, $p < 0.001$) and defensive motivation on maladaptive response ($\beta = 0.495$, $t = 4.563$, $p < 0.001$), supporting H5 and H6. However, no significant moderation effect was found either for the relationship between response efficacy and protection motivation, or self-efficacy and defensive motivation. Overall, this explained ~33.5% of the variance in protection motivation, ~41.5% of the variance in defensive motivation, ~22.4% of the variance in adaptive response, and ~26.8% of the variance in maladaptive response. According to Cohen's (2013) benchmark range, these variances are satisfactory. The results are summarized in Table 7. The structural equation modeling analysis provided an answer to the first research question: that consumers' adaptive and maladaptive responses are driven by the two dimensions of perceived efficacy of external cues, response efficacy and self-efficacy, respectively. Unfortunately, the moderation effect of perceived threat on the relationships between perceived efficacy and protection/defensive motivation was not confirmed by the current data set.

Figure 2. Path coefficients



Control variables were included in the model. The previous literature suggests that consumers' age, gender, education, use duration and prior experience in using the internet or mobile services may affect their attitudes toward privacy (Wottrich et al., 2018; Xu et al., 2012). Apart from these, monthly income and frequency were identified as potential factors that influence consumers' actual behavior, which may be highly related to consumers' familiarity with emerging online markets. However, none of these control variables were found to be significant based on the current data set. It seems that the control factors contributing to attitudes about privacy cannot be applied to the actual behaviors.

Table 7. Significance test results

Path	H#	COEF	*t*-value	*p*-value	Results
RESP –> PM	H1	0.327	3.278	0.001 (**)	Supported
SEFF –> DM	H2	0.524	6.723	0.000 (***)	Supported
TSUS* RESP –> PM	H3	0.097	0.836	0.403	Not supported
TSEV* SEFF –> DM	H4	–0.200	1.384	0.178	Not supported
PM –> AR	H5	0.386	3.616	0.000 (***)	Supported
DM –> MR	H6	0.495	4.563	0.000 (***)	Supported

Notes: (a) Key: RESP: response efficacy, PM: protection motivation, SEFF: self-efficacy, DM: defensive motivation, TSUS: perceived susceptibility, TSEV: perceived severity, AR: adaptive response, MR: maladaptive response; (b) Significance level: ***p < 0.001, **p < 0.01, *p < 0.05.

Experiment Discussion

Based on the above, in the untreated base group (Group #4), consumers' response efficacy had a positive relationship with their protection motivation, and their self-efficacy had a positive relationship with their defensive motivation. The effect of protection motivation on adaptive responses and the effect of defensive motivation on maladaptive responses were also significant. It seems that generally, individuals' perceived efficacy in dealing with potential threats motivates their behavior responses sufficiently.

For the danger control process, in Group #1, respondents were manipulated with messages about personal data that had been collected and sold to third parties. Only one significant path between consumers' protection motivation and adaptive responses was found ($\beta = 0.505$, $t = 3.493$, $p < 0.001$). In Group #2, respondents were exposed to message content stating that personal data were collected but not sold to any third party. No path was found as significant with this condition. In Group #3, respondents were exposed to message content stating that personal data were sold to a third party but with no mention of data collection. Here, a significant path is apparent between consumers' response efficacy and their protection motivation ($\beta = 0.605$, $t = 3.905$, $p < 0.001$), as well as the path between protection motivation and adaptive response ($\beta = 0.502$, $t = 4.911$, $p < 0.001$). For the fear control process, Group #1, no path was found as significant in this condition. This was the same for Group #2. In Group #3, the path between consumers' self-efficacy and their defensive motivation ($\beta = 0.573$, $t = 4.574$, $p < 0.001$) was significant.

Obviously, after being informed about the misuse of personal data, respondents were affected to some degree, and this is manifested in the lack of significance in previously significant relationships. Compared with the danger control process, the changes in respondents' perceptions and actions in the fear control process were greater. In all three treatment groups, the relationship between consumers' defensive motivations and maladaptive responses was no longer significant, and only Group #3 displayed a weaker but still significant path between consumers' self-efficacy and their defensive motivations. This indicates that, when hearing news about their personal data being misused, consumers' confidence in their own ability to protect themselves from privacy threats was not enough to trigger their defensive motivation as well as a maladaptive response. Conversely, in the danger control process, the relationship between consumers' response efficacy and protection motivation, and the subsequent adaptive response in the treatment group did not change that much in the base group. This implies that, when learning news about their personal data being misused, consumers' faith in the effectiveness of prospective measures taken to protect their personal data was still sufficient to inspire a protection motivation and adaptive response, as expected.

Regarding the different types of reported misuse of personal information (personal data being collected by vs. personal data being sold to third parties), it seemed that, compared with the base group, minimal changes in reaction were caused when consumers were exposed to the reported misuse of personal data being sold to third parties; a medium change was caused when consumers were exposed to personal data being collected and then sold to third parties; a maximal change was caused when consumers were exposed to personal data being collected by third parties. Assuming that respondents in the base group were less concerned about privacy, because no manipulation was used here, a possible explanation for changes in the other groups might be that consumers believed a privacy invasion would induce a much more serious problem if their data were collected, rather than if sold to third parties. This makes sense because personal data being collected can be re-sold or re-used, which is a more fluid situation than personal data being sold. In other words, to maintain consumers' adaptive responses and decrease their maladaptive responses in a practical way, the misuse of personal data (being sold) should be reported preferentially over other types of misuse. However, this is speculation and further investigation is required to corroborate these findings.

PRACTICAL IMPLICATIONS

This study reveals several important practical implications. First, it is set in the online marketing environment. The notion of information privacy has recently been viewed as a critical issue that deserves attention from both scholars and practitioners. Successfully addressing information privacy issues is particularly relevant to business growth in the information age. This is especially true for emerging online markets because their success and the quality of their customer service largely hinge on their ability to collect and analyze a vast amount of consumers' personal data. This study investigates consumers' responses to information practices in the context of emerging online markets.

Second, as people become aware of threats to privacy, they begin to demand that online platforms should employ countervailing protective measures around personal data. In response, regulatory stakeholders may mandate the necessary deployment of regulations to alleviate consumer privacy concern while meeting the needs of developing online markets. The results of this study can offer insights and inspire regulatory stakeholders regarding which type of personal data misuse to identify.

Third, this study addresses the problems that arise with individual-level privacy protection in emerging online markets. Some deficiencies are entrenched in the privacy regulations and have been exposed in practical use, such as the need for more effectively designed misuse-reporting mechanisms. Based on the results obtained, the type of reported misuse of personal data should be selected to balance consumer protection while not harming online markets.

Finally, while legislative institutions and the mass media routinely discuss the importance of privacy protection, there is an absence of academic debate on the formulation of proper regulation that considers psychological and economic rationales. For example, is it necessary for privacy regulations to strictly restrict online platforms in their information acquisition to protect consumers? If the answer is "yes," to what extent should restrictions be applied? This study can offer some insights regarding these questions from a consumer perspective.

LIMITATIONS AND FUTURE RESEARCH DIRECTION

This study still has several limitations, which future research can address. First, more than 60% of the subjects had no income, and with more than 50%, their use frequency is quite low. This limitation is mainly because student samples were involved in the experiments. On the one hand, student samples represent a major force of online service users, which should be considered. On the other hand, their behavior reaction to privacy might differ to other income groups. Further tests with different subjects should be conducted to validate the current results. Next, a significant future research direction lies in the theoretical extension of the extended parallel process model. It failed to prove the moderation role that perceived threat plays in stimulating parallel reactions. The insufficiency of the manipulated text messages used in the experiment may account for this. Therefore, it vital to refine the experiment design and re-test the proposed model with respect to different situations. Additionally, the effect of negatively valenced emotional arousal has not been considered in the proposed research model. Future research could be conducted to fill this gap. Moreover, further issues, such as at what occasion, or in what way the misuse of personal data should be reported, needs exploration, as this may offer comprehensive insights for practical applications.

ACKNOWLEDGMENT

The authors thank the Editors and the three anonymous reviewers for their valuable comments that help improve the paper substantially. This research was partially supported by the XJTLU IBSS Development Fund [grant number IBSSDF-0121-29], and by the Innovation and Entrepreneurship Program of Jiangsu Province [grant numbers JSSCBS20210763, JSSCBS20210768].

REFERENCES

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509–514. doi:10.1126/science.aaa1465 PMID:25635091

Adjerid, I., Acquisti, A., Telang, R., Padman, R., & Adler-Milstein, J. (2016). The impact of privacy regulation and technology incentives: The case of health information exchanges. *Management Science*, *62*(4), 1042–1063. doi:10.1287/mnsc.2015.2194

Adjerid, I., Peer, E., & Acquisti, A. (2018). Beyond the privacy paradox: Objective versus relative risk in privacy decision making. *Management Information Systems Quarterly*, *42*(2), 465–488. doi:10.25300/MISQ/2018/14316

Andrew, J., & Baker, M. (2019). The general data protection regulation in the age of surveillance capitalism. *Journal of Business Ethics*, *168*(3), 565–578. doi:10.1007/s10551-019-04239-z

Anic, I. D., Škare, V., & Milaković, I. K. (2019). The determinants and effects of online privacy concerns in the context of e-commerce. *Electronic Commerce Research and Applications*, *36*, 100868. Advance online publication. doi:10.1016/j.elerap.2019.100868

Banerjee, S., Hemphill, T., & Longstreet, P. (2018). Wearable devices and healthcare: Data sharing and privacy. *The Information Society*, *34*(1), 49–57. doi:10.1080/01972243.2017.1391912

Boss, S., Galletta, D., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *Management Information Systems Quarterly*, *39*(4), 837–864. doi:10.25300/MISQ/2015/39.4.5

Brehm, S. S., & Brehm, J. W. (1981). *Psychological reactance: A theory of freedom and control*. Academic Press.

Budak, J., Rajh, E., & Anić, I. D. (2015). Privacy concern in Western Balkan countries: Developing a typology of citizens. *Journal of Balkan & Near Eastern Studies*, *17*(1), 29–48. doi:10.1080/19448953.2014.990278

California Consumer Privacy Act. (n.d.). https://en.wikipedia.org/wiki/California_Consumer_Privacy_Act

Chang, H. H., & Wong, K. H. (2018). Consumer psychological reactance to coalition loyalty program: Price-consciousness as a moderator. *Service Business*, *12*(2), 379–402. doi:10.1007/s11628-017-0353-6

Chellappa, R. K., & Shivendu, S. (2007). An economic model of privacy: A property rights approach to regulatory choices for online personalization. *Journal of Management Information Systems*, *24*(3), 193–225. doi:10.2753/MIS0742-1222240307

De Hoog, N., Stroebe, W., & De Wit, J. B. (2007). The impact of vulnerability to and severity of a health risk on processing and acceptance of fear-arousing communications: A meta-analysis. *Review of General Psychology*, *11*(3), 258–285. doi:10.1037/1089-2680.11.3.258

Dogruel, L., Joeckel, S., & Vitak, J. (2017). The valuation of privacy premium features for smartphone apps: The influence of defaults and expert recommendations. *Computers in Human Behavior*, *77*, 230–239. doi:10.1016/j.chb.2017.08.035

Endler, N. S., & Parker, J. D. (1990). Multidimensional assessment of coping: A critical evaluation. *Journal of Personality and Social Psychology*, *58*(5), 844–854. doi:10.1037/0022-3514.58.5.844 PMID:2348372

Fair Information Principles. (n.d.). https://en.wikipedia.org/wiki/FTC_fair_information_practice

General Data Protection Regulation. (2018). https://gdpr-info.eu/

Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security*, *77*, 226–261. doi:10.1016/j.cose.2018.04.002

Ginosar, A., & Ariel, Y. (2017). An analytical framework for online privacy research: What is missing? *Information & Management*, *54*(7), 948–957. doi:10.1016/j.im.2017.02.004

Hong, W., Chan, F. K. Y., & Thong, J. Y. L. (2019). Drivers and inhibitors of internet privacy concern: A multidimensional development theory perspective. *Journal of Business Ethics*, *168*(3), 539–564. doi:10.1007/s10551-019-04237-1

Hui, K. L., Teo, H. H., & Lee, S. Y. T. (2007). The value of privacy assurance: An exploratory field experiment. *Management Information Systems Quarterly*, *31*(1), 19–33. doi:10.2307/25148779

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *Management Information Systems Quarterly*, *34*(3), 549–566. doi:10.2307/25750691

Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *Management Information Systems Quarterly*, *39*(1), 113–134. doi:10.25300/MISQ/2015/39.1.06

Langenderfer, J., & Cook, D. L. (2004). Oh, what a tangled web we weave: The state of privacy protection in the information economy and recommendations for governance. *Journal of Business Research*, *57*(7), 734–747. doi:10.1016/S0148-2963(02)00359-4

Leventhal, H. (1970). Findings and theory in the study of fear communications. *Advances in Experimental Social Psychology*, *5*, 119–186. doi:10.1016/S0065-2601(08)60091-X

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *Management Information Systems Quarterly*, *33*(1), 71–90. doi:10.2307/20650279

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, *11*(7), 394–413. doi:10.17705/1jais.00232

Liu, Y., & Du, R. (2020). Examining the effect of reviewer socioeconomic status disclosure on customers' purchase intention. *Journal of Global Information Management*, *28*(3), 17–35. doi:10.4018/JGIM.2020070102

Lonkani, R., Changchit, C., Klaus, T., & Sampet, J. (2020). A comparative study of trust in mobile banking: An analysis of US and Thai customers. *Journal of Global Information Management*, *28*(4), 95–119. doi:10.4018/JGIM.2020100106

Lwin, M., Wirtz, J., & Williams, J. D. (2007). Consumer online privacy concerns and responses: A power–responsibility equilibrium perspective. *Journal of the Academy of Marketing Science*, *35*(4), 572–585. doi:10.1007/s11747-006-0003-3

Miltgen, C. L., & Smith, H. J. (2015). Exploring information privacy regulation, risks, trust, and behavior. *Information & Management*, *52*(6), 741–759. doi:10.1016/j.im.2015.06.006

Nam, T. (2019). What determines the acceptance of government surveillance? Examining the influence of information privacy correlates. *The Social Science Journal*, *56*(4), 530–544. doi:10.1016/j.soscij.2018.10.001

Oppenheimer, D. M., Meyvis, T., & Davidenko, N. (2009). Instructional manipulation checks: Detecting satisficing to increase statistical power. *Journal of Experimental Social Psychology*, *45*(4), 867–872. doi:10.1016/j.jesp.2009.03.009

Personal Information Protection and Electronic Documents Act. (2004). https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

Popova, L. (2012). The extended parallel process model: Illuminating the gaps in research. *Health Education & Behavior*, *39*(4), 455–473. doi:10.1177/1090198111418108 PMID:22002250

Preibusch, S., Peetz, T., Acar, G., & Berendt, B. (2016). Shopping for privacy: Purchase details leaked to PayPal. *Electronic Commerce Research and Applications*, *15*, 52–64. doi:10.1016/j.elerap.2015.11.004

Rahman, M. S., Hossain, M. A., Zaman, M. H., & Mannan, M. (2020). E-Service quality and trust on customer's patronage intention: Moderation effect of adoption of advanced technologies. *Journal of Global Information Management*, *28*(1), 39–55. doi:10.4018/JGIM.2020010103

Rogers, R. W., & Deckner, C. W. (1975). Effects of fear appeals and physiological arousal upon emotion, attitudes, and cigarette smoking. *Journal of Personality and Social Psychology*, *32*(2), 222–230. doi:10.1037/0022-3514.32.2.222 PMID:1107512

Rosenberg, B. D., & Siegel, J. T. (2018). A 50-year review of psychological reactance theory: Do not read this article. *Motivation Science*, *4*(4), 281–300. doi:10.1037/mot0000091

Ruiter, R. A., Kessels, L. T., Peters, G. J. Y., & Kok, G. (2014). Sixty years of fear appeal research: Current state of the evidence. *International Journal of Psychology*, *49*(2), 63–70. doi:10.1002/ijop.12042 PMID:24811876

Sánchez, D., & Viejo, A. (2017). Personalized privacy in open data sharing scenarios. *Online Information Review*, *41*(3), 298–310. doi:10.1108/OIR-01-2016-0011

Schneier, B. (2015). *Data and Goliath: The hidden battles to collect your data and control your world*. WW Norton.

Sengupta, S. (2020). How does culture impact customer evaluation in online complaining? Evidence from Germany and India. *Journal of Global Information Management*, *28*(2), 131–159. doi:10.4018/JGIM.2020040107

Van Ooijen, I., & Vrabec, H. U. (2019). Does the GDPR enhance consumers' control over personal data? An analysis from a behavioural perspective. *Journal of Consumer Policy*, *42*(1), 91–107. doi:10.1007/s10603-018-9399-7

Wang, J., Li, Y., & Rao, H. R. (2017). Coping responses in phishing detection: An investigation of antecedents and consequences. *Information Systems Research*, *28*(2), 378–396. doi:10.1287/isre.2016.0680

Westin, A. F. (1967). *Privacy and freedom*. Atheneum.

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communication Monographs*, *59*(4), 329–349. doi:10.1080/03637759209376276

Witte, K. (1994). Fear control and danger control: A test of the extended parallel process model (EPPM). *Communication Monographs*, *61*(2), 113–134. doi:10.1080/03637759409376328

Witte, K., & Allen, M. (2000). A meta-analysis of fear appeals: Implications for effective public health campaigns. *Health Education & Behavior*, *27*(5), 591–615. doi:10.1177/109019810002700506 PMID:11009129

Wottrich, V. M., van Reijmersdal, E. A., & Smit, E. G. (2018). The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness, and privacy concerns. *Decision Support Systems*, *106*, 44–52. doi:10.1016/j.dss.2017.12.003

Wu, P. F., Vitak, J., & Zimmer, M. T. (2019). A contextual approach to information privacy research. *Journal of the Association for Information Science and Technology*, *71*(4), 485–490. doi:10.1002/asi.24232

Xu, H., Teo, H. H., Tan, B. C., & Agarwal, R. (2009). The role of push-pull technology in privacy calculus: The case of location-based services. *Journal of Management Information Systems*, *26*(3), 135–174. doi:10.2753/MIS0742-1222260305

Xu, H., Teo, H. H., Tan, B. C. Y., & Agarwal, R. (2012). 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*, *23*(4), 1342–1363. doi:10.1287/isre.1120.0416

Chenwei Li is an Assistant Professor of International Business School Suzhou, Xi'an Jiaotong-Liverpool University. She obtained her PhD degree from Faculty of Business and Economics, The University of Hong Kong. Her research interests focus on Information Security and Privacy, Human-Computer Interaction, E-Commerce and Consumer Behavior as well as Information Dissemination.

Jie Chu is an Assistant Professor in the International Business School Suzhou (IBSS) at Xi'an Jiaotong-Liverpool University. He obtained his Ph.D. degree in Management Science from DeGroote School of Business, McMaster University. His research interests focus on the applications of optimization approaches to supply chain management decisions. Prior to joining the IBSS, Dr. Chu has worked as an Assistant Professor in College of Economics and Management at Huazhong Agricultural University.

Leven J. Zheng is an Assistant Professor in Management at the Department of Global Business and Marketing, Hong Kong Metropolitan University. He Received his Ph.D. in Innovation and Entrepreneurship from the Management School at the University of Liverpool. His research interests focus on entrepreneurship, newly public firms, new product development, entrepreneurial founding team or senior management team as well as entrepreneurial internationalization. His research has appeared in Journal of Business Research, Technovation, and Technological Forecasting & Social Change. He uses both qualitative and quantitative research methods. He also serves as an Entrepreneurship Counsellor for ChuangPlus (student) entrepreneurship incubator at Tsinghua University, P.R.China, and an Entrepreneurship and Innovation Mentor at Suzhou Mudu Economic Development Zone and Suzhou Wuzhong Science and Technology Park, P.R. China.

APPENDIX

Table 8. Cross-loading on the Constructs

Construct	Item	Perceived Severity	Perceived Susceptibility	Self-Efficacy	Response Efficacy	Protection Motivation	Defensive Motivation	Adaptive Response	Maladaptive Response
Perceived Severity	TSEV1	0.866	0.371	0.158	0.264	0.263	0.166	0.177	0.121
	TSEV2	0.947	0.585	0.193	0.380	0.395	0.252	0.298	0.098
	TSEV3	0.968	0.535	0.218	0.378	0.382	0.289	0.271	0.140
Perceived Susceptibility	TSUS1	0.488	0.934	0.200	0.233	0.401	0.243	0.402	0.065
	TSUS2	0.526	0.974	0.234	0.199	0.449	0.221	0.412	0.041
	TSUS3	0.553	0.945	0.218	0.221	0.398	0.201	0.427	0.018
Self-Efficacy	SEFF1	0.178	0.256	0.903	0.444	0.320	0.542	0.290	0.259
	SEFF2	0.201	0.226	0.921	0.525	0.315	0.496	0.347	0.251
	SEFF3	0.187	0.145	0.905	0.511	0.250	0.600	0.270	0.354
Response Efficacy	RESP1	0.347	0.224	0.513	0.964	0.424	0.435	0.221	0.258
	RESP2	0.388	0.245	0.536	0.974	0.422	0.436	0.271	0.249
	RESP3	0.349	0.191	0.519	0.956	0.425	0.417	0.242	0.211
Protection Motivation	PM1	0.358	0.418	0.282	0.367	0.903	0.310	0.370	0.122
	PM2	0.351	0.338	0.343	0.503	0.921	0.414	0.300	0.238
	PM3	0.347	0.452	0.269	0.345	0.936	0.324	0.393	0.158
Defensive Motivation	DM2	0.292	0.265	0.571	0.466	0.402	0.963	0.307	0.477
	DM3	0.212	0.183	0.588	0.390	0.327	0.961	0.239	0.476
Adaptive Response	AR1	0.294	0.425	0.200	0.153	0.276	0.236	0.817	-0.273
	AR2	0.269	0.404	0.178	0.158	0.299	0.133	0.834	-0.328
	AR3	0.124	0.242	0.395	0.284	0.348	0.305	0.770	0.057
Maladaptive Response	MR1	0.119	0.050	0.353	0.294	0.184	0.507	-0.208	0.942
	MR2	0.117	0.029	0.219	0.148	0.158	0.396	-0.171	0.904