Accepting Privacy Scheme in the Presence of Consumer Privacy Fatalism: The Elaboration Likelihood Model and Fear Appeals

Early stage research

Bright Frimpong
University of Texas Rio Grande Valley
bright.frimpong01@utrgv.edu

Emmanuel W. Ayaburi
University of Texas Rio Grande Valley
emmanuel.ayaburi@utrgv.edu

Francis Kofi Andoh-Baidoo,
University of Texas Rio Grande Valley,
francis.andohbaidoo@utrgv.edu

Jae Ung Lee
Louisiana Tech University,
jakelee@latech.edu

Abstract

A major concern with privacy is consumer privacy fatalism, or the belief that the consumers believe they have little control over their privacy online. Based on the elaboration likelihood model (ELM) and fear appeals, the study proproses an integrated model that seeks to reduce consumer privacy fatalism and subsequently, influences consumer decision to opt-in for a privacy scheme. The study will use an online experimental vignette to investigate the research problem. The study will contribute to unraveling the relationship between fatalistic views and privacy precautionary behaviors and unveil the boundary conditions of ELM and fear appeals in the context of fatalistic attitude change. Furthermore, the findings will help inform the decision to promote opt-in or opt-out as privacy experts push to empower consumers.

Keywords: Consumer privacy fatalism, fear appeals, elaboration likelihood, opt-in, privacy schemes.

Introduction

The perception that individual privacy boundaries cannot be controlled seems to be gaining traction among online consumers. A recent survey of online consumers in the U.S and U.K. revealed that the proportion of people who agreed to the statement "online privacy is possible" had decreased from 61% to 32% respectively (Greg 2019). The 50% reduction demonstrates the mistrust or lack of belief in the introduction of tools such as personalization features aimed at providing consumers more autonomy in managing their privacy boundaries. Such consumers are described as privacy fatalists because of their beliefs that there is little that can be done to ensure proper use of personal information (Sheung-Hung and Wailoon 2013). Consumers with such beliefs may make any efforts toward increased privacy protection futile due to apathy or lack of involvement in privacy protection programs (Rule, 2007). For instance, while several privacy tools and settings (e.g., TRUSTe, P3P, OPA) have been developed to help protect online consumer privacy, privacy fatalists are likely to avoid using them because of their perceived sense of powerlessness. Privacy fatalists will rather choose to be vulnerable to privacy risks than take any precautionary action. Such behavior perpetuates the cycle of privacy risk in what is termed rational fatalism (Kerwin, 2012).

The focus of this study is on the evolving concepts of privacy schemes or personalization where consumers are encouraged to opt-in a privacy policy or use a tool that promises greater protection. The decision to opt into or use privacy tools is riskier as the subsequent outcomes are uncertain (Franklin et al. 2007; Guthrie et al. 2014; Xie et al, 2019). Thus, privacy fatalistic beliefs adversely influence the use/efficacy of privacy protection technologies and reduce such technology to incomplete and ineffective tools (Furnell and Clarke, 2012).

Recognizing the need to change consumer behavior, information systems research has investigated behavior change interventions aimed at promoting precautionary behaviors. Behavior change interventions refer to a coordinated set of activities designed to change specified behavior patterns (Michie et al, 2011). Previous studies have identified four different types of behavior change interventions that can be adopted to promote precautionary behavior: security education, training, awareness-raising, and design of technical tools (Kirlappos and Sasse 2012; Posey et al., 2015). These interventions have widely been adopted in several employee and workplace security studies and form the basis for the security, education, training,

and awareness program (SETA). The education component entails developing and understanding the knowledge required to identify and mitigate security threats while the training component involves developing the needed information security skills. Awareness-raising involves the use of warning messages containing threats and countermeasures while design involves the nudges in the environment that urges individuals to perform security actions (Jansen and van Schaik, 2019).

This study adapts the awareness-raising component of the SETA interventions and investigates its impact on consumers' privacy fatalism. The underlying assumption of SETA programs is that consumer alertness and motivation can be manipulated to achieve the desired outcome. Thus, this study poses the following question: *1) can online consumers be persuaded to change their privacy fatalistic beliefs? and 2) will the decision toward privacy schemes be influenced by underlying privacy fatalistic beliefs associated with their use?*

Prior information systems research has used the elaboration likelihood model (ELM) and fear appeals as the theoretical lens to understand how users' attitudes towards security and privacy issues change over time (Wall and Warkentin 2019; Keller and Block 1996; Johnston et al. 2015). Drawing on these two theoretical foundations, the study conducts a quasi-behavioral experiment that tests the interactive effect of threats and persuasion routes to persuade consumers to opt into privacy schemes by reducing their privacy fatalistic beliefs. The study will recruit online consumers who prophesy to having fatalistic beliefs about privacy into four experimental conditions (high threat, low threat, objective processing route, and imagery processing route). The experiment will assess the effect of fear and persuasion on the relationship between fatalistic beliefs and the likelihood of opting into privacy programs.

This study will make contributions to the awareness-raising component of the SETA interventions and provide insights for privacy managers. People with high fatalistic views have been found to take fewer steps to protect both informational and social privacy on the internet (Xie et al. 2019). The findings from the research will help unravel the logical inverse relationship between fatalistic views and privacy precautionary behaviors. The results will help unveil the boundary conditions of ELM and fear appeals in the context of fatalistic attitude change. Furthermore, the findings will help inform the decision to promote opt-in or opt-out as privacy experts push to empower consumers. Finally, practical insights gleaned from the study findings will contribute to design pragmatic SETA programs.

Background Literature

Two key streams of literature inform this study are; 1) consumer fatalistic belief about privacy and 2) the decision to accept privacy programs or schemes offered by firms. To understand the state of the literature, the next section discusses the literature on the two streams.

Consumer Privacy Fatalism

Individuals normally express concern for their online privacy, however, recent studies have found that such "concerned" individuals most often fail to adopt privacy schemes or voluntarily engage in information disclosure activities (Yao and Daniel, 2008; Xie et al, 2019). This phenomenon describes the dichotomy between the privacy concerns of people and their actual behavior. Several theoretical explanations from diverse disciplines have been provided to clarify this dichotomy between consumers' attitudes and behavior towards information privacy. Previous studies have sought to explain this paradox from a social theory perspective, using theories such as the privacy calculus theory (Culnan and Armstrong, 1999), structuration theory (Zafeiropoulou et al., 2013), media theories (Debatin et al., 2009), communicative privacy management theory (Lee et al., 2013), gemeinschaft/gesellschaft theory (Stutzman et al., 2012), and the theory of social representation (Oetzel and Gonja, 2011). In spite of all these theories, no single theoretical model has prevailed and as such, there still remains room for additional theoretical perspectives. One philosophical theory that purports to offer a fresh outlook on the paradox is the rational fatalism, which argues that rational people may take more risks when the danger inherent in those risks becomes unavoidable (Kerwin 2012).

Several authors have offered various definitions of rational fatalism, such as "passively denying personal control" (Neff and Hoppe, 1993) and "expressing an attitude of resignation in the face of events that are thought to be inevitable" (Powe and Johnson, 1995). This phenomenon has been applied in several research areas like health communication, food safety issues, adolescent unemployment, and psychological distress. Fatalism has also been associated with risky sexual behaviors (Beltrán et al. 1993), depression (Neff and Hoppe, 1993), and demographic variables such as social-economic status (Roberts et al. 2000). Further, fatalism has widely been used in research studies concerning public health behavior and decision-making. Such studies have often produced interesting theories and results. For instance, one such theory is cancer

fatalism, which explains why some cancer patients forgo cancer screenings or refuse a recommended course of treatment (Gregg and Curry 1994). Powe and Finnie (2003) assert that this behavior is borne out of the belief that death is inevitable when cancer is present and as such being healthy is beyond one's control and purely, a matter of fate or luck.

In the attempt to conceptualize fatalism, previous studies have identified numerous dimensions including helplessness, pessimism, luck, internality, inevitability, and divine control (Esparza, Wiebe, and Quiñones 2015; Shen, Condit, and Wright 2009). Other studies have also identified similar dimensions including locus of control (Joiner et al.2001; Wade 1996), learned helplessness (Clarke, MacPherson, and Holmes 1982) and pessimism (Scheier and Bridges 1995). Due to the numerous divergent dimensions of fatalism, there is no universally accepted scale to measure the construct. However, some authors have argued that "helplessness" is the most important dimension and has used it to operationalize fatalism (Franklin et al. 2007; Guthrie et al. 2014; Xie et al, 2019).

Xie et al (2019) adapted the theory of fatalism to online information privacy research. Their study also operationalized fatalism on the "helplessness" dimension and sought to measure rational privacy fatalism from three viewpoints: fatalism about legal protections of privacy, fatalism about technology's ability to protect privacy, and fatalism about businesses ability to protect private information. The study investigated the extent to which people were fatalistic about their online privacy and the relationship between rational fatalism and a section of demographic variables. They found that participants held relatively high level of fatalistic beliefs in technology and businesses ' ability to protect their privacy. Although results on fatalism about legal protections of privacy were inconclusive, most participants exhibited some form of fatalism towards the law. Nevertheless, the study empirically demonstrated the existence of privacy fatalism and its impact on privacy precautionary behavior. The authors concluded that privacy fatalistic people are very vulnerable to privacy threats since they are likely to ignore privacy measures due to their belief that their risk of online privacy is already predetermined. Hence, the motivation for this study to determine whether the use of persuasion/threat-inspired privacy schemes (awareness-raising intervention) will lead to a reduction in consumer fatalistic beliefs.

Privacy Scheme Awareness

Privacy protection relies on the actions and inactions of individuals, organizations, and policy-regulators. Individual privacy protection depends on individuals' awareness of the risks of disclosing personal information aimed at encouraging precautionary behaviors (Pötzsch, 2008). Awareness is generally based on the individual's attention, perception, and cognition of tangible and intangible objects in the surrounding environment (Correia and Compeau 2017). Privacy awareness depends on how an individual is informed about privacy practices and policies (Dunfee et al. 1999; Phelps et al. 2000; Ermakova et al., 2014). Privacy awareness is an essential prerequisite for individuals to make informed decisions about whether or not to engage in precautionary behaviors such as data disclosure or the use of privacy settings. The construct captures an individual's knowledge of possible privacy threats, violations, and potential solutions.

Previous research has found awareness to be a significant motivator for precautionary and security behavior (Karjalainen and Siponen 2011; Puhakainen and Siponen 2010). For instance, Boss et al. (2009) reported that increased policy awareness motivated user compliance and proactive precautionary behavior. However, a study by Govani and Pashley (2005) found that creating awareness for privacy issues were not sufficient motivators for precautionary behaviors. The authors noted that privacy disclosure on Facebook was not significantly reduced after informing users of the potential privacy risks. These findings represented a deviation from the expected objectives which was to use privacy awareness as a motivating tool for people to either engage in precautionary behaviors or change their disclosure preferences. Further, Vemou and Karyda (2013) argue that awareness of privacy tools is weakly correlated to their adoption and usage even though awareness is an essential prerequisite for the usage of privacy tools.

Security policy is rendered ineffective if it fails to ensure user security compliance and precautionary behaviors (Puhakainen and Siponen, 2010). Therefore, the key to ensuring the efficacy of a security policy is to create awareness in a manner that motivates user compliance and precautionary behaviors. As such, previous studies have often relied on experimental manipulations of both high and low fear appeals to create awareness (Milne et al. 2000). This approach provides a base-level awareness of a threat and allows researchers to reinforce threat awareness using different levels of fear appeals. Researchers can then

measure which level of fear appeal elicits the desired fear or response from participants. Based on the desired fear or response, an awareness intervention can then be designed using the appropriate level of fear appeal. This demonstrates the importance of fear appeals in the design of security and privacy awareness interventions.

Limited research attention has been given to fear and fear appeals in the InfoSec domain (Johnston et al. 2015). Also, the idea that individuals may engage in different levels of fear appeal elaboration has not been fully explored in the InfoSec literature. Wall and Warkentin (2019) argue that the theoretical underpinnings of persuasion theories such as the ELM and HSM make it possible to gain deeper insights into the design of fear appeal messages. For instance, perceived argument quality has been found to improve the efficacy of messages delivered in security training (Puhakainen and Siponen 2010). Therefore, the authors assert that perceived argument quality of a fear appeal message should provide a partial explanation for the effectiveness of the fear appeal message (Wall and Warkentin 2019). Logically, it can also be assumed that individuals' perceptions of the quality of a threat message regarding the threat's severity and their susceptibility to the threat should also have an influence on their attitude towards the threat. Findings from Keller and Block (1996) provide empirical support for this assumption. Results from the 1996 study indicate that a fear appeal message does not have a direct influence on persuasion but rather, provokes an elaboration of the message which then affects persuasion.

Fear appeals and protection motivation theory (PMT) together with the elaboration likelihood model (ELM) are persuasion-based theories that have been adopted and applied in behavioral studies in information security research. The PMT has been used in literature to demonstrate that fear appeals are effective in promoting precautionary motivations and privacy protection behaviors (Wall and Buche, 2017; Herath and Rao, 2009). Likewise, we expect the results to provide both theoretical and practical insights on which of the factorial combinations of fear appeals (high and low) and elaboration routes (objective and imagery processing) have the most impact on reducing consumers' privacy fatalism.

Although it is important for users to be aware of the existence of privacy tools, there is also the need for further interventions post-awareness to motivate users to adopt these schemes for privacy protection. Vemou and Karyda (2013) recommend that researchers should study the behavioral and technical issues which cause the disconnect between privacy schemes awareness and their usage. This study addresses

privacy fatalism, a behavioral issue which has a negative impact on users' attitude to privacy schemes. We propose the need for an intervention aimed at reducing privacy fatalism which should indirectly facilitate the transition from the awareness of a privacy scheme to their adoption/opt-in.

Theoretical Development

Fear Appeals

The protection motivation theory (PMT) asserts that, when faced with a threatening event, individuals engage in two appraisal process: threat and coping appraisal. The threat appraisal focuses on the threat itself and nudges the individual to consider both the gravity of the consequences of the threat (perceived severity) and the probability of the threat occurring (perceived susceptibility). Meanwhile, the coping appraisal focuses on the individual's ability to act against the threat. This involves evaluating whether a recommended course of action will neutralize the threat (response efficacy) and also, assessing the perceived level of confidence one possesses to carry out the recommended course of action (self-efficacy). Threat appraisal and fear appeals have been used interchangeably in the PMT literature (Jansen and van Schaik, 2019), however, this study will resort to the use of fear appeals for consistency. Millne et al. (2000) assert that "when PMT is used as a theoretical basis for interventions, the focus is on the operation of fear appeals". This is because PMT provides the theoretical framework to predict peoples' intention to protect themselves after exposure to fear appeal interventions.

This study focuses on the fear appeal component of the PMT. Fear appeals involve the use of persuasive messages containing information about a threat to persuade people to embrace certain intentions and actions. Persuasive communcations have been found to be an effective method for modifying human attitutedes, intentions and behaviors (Fishbein and Ajzen, 1975). Wall and Warkentin (2019) echo the need for future research to evaluate the message design of fear appeals to develop more effective fear-appeal interventions. This has become necessary due to the inconsistencies in the literature regarding the efficacy of fear appeals. Also, fear appeals with poor designs are likely to be ineffective in provoking the desired response. Effective fear appeals do not only present the threat but also provide solutions that fall within users' coping ability (Witte and Allen 2000).

According to Witte (1992), a fear appeal has two parts. The first part comprises the severity and certainity of the threat whereas the second part captures the response efficacy and self efficcay Needless to say, equal attention ought to be put on both parts when designing fear appeals so as to address the privacy risk and the individual's ability to respond to it. A well-designed fear appeal should inspire individuals to engage in both threat and coping appraisal leading to the desired protective response rather than message avoidance or rejection.

Elaboration Routes

The ELM is a theory of persuasion developed by Cacioppo and Petty (1979) to explain the observed differences in the amount of cognitive energy people devote to persuasive messages. When a persuasive message is presented to an individual, a level of elaboration occurs. Elaboration refers to the amount of cognitive effort used by an individual to process and evaluate a persuasive message. When people are exposed to new information, their level of elaboration depends on two factors: motivation and ability. The ELM uses an individual's level of motivation and ability to predict which route will be chosen to process a persuasive message. Individuals have been found to process information through the central and peripheral processing routes. Research shows that highly motivated individuals who are able to evaluate persuasive messages use the central processing route (Cacioppo and Petty 1979). The central processing route is often considered as the logical and elaborate route due to the amount of cognitive energy required for deep information processing and critical judgment. Individuals use this route when they care about the message and therefore are willing to engage in a high level of elaboration. However, individuals lacking motivation and ability to evaluate persuasive messages engage the peripheral processing route. In the peripheral route, individuals do not use any cognitive energy or logic but rather rely on environmental characteristics and heuristics to evaluate the message. This happens when individuals do not care about the message and therefore engage in a low level of elaboration. This study adapts the elaboration routes used in Keller and Block (1996) where imagery and objective processing are used to represent peripheral and central cues respectively. Keller and Block studied the use of arousal and elaboration to increase the persuasiveness of fear appeals. They found that the level of fear arousal was positively associated with the propensity to

elaborate. Thus, a high-fear appeal provoked higher levels of elaboration when compared to a low-fear appeal.

Other studies have also looked at the effects of ELM on precautionary behavior. For instance, Johnston and Warkentin (2010) found that the source credibility of the security message sender influences employee's security behaviors and intentions. Higher levels of perceived argument quality have also been found to improve individuals' perception of response efficacy and their intention to comply with security policies (Wall and Warkentin 2019). Studies that have adapted an integrated-theory approach using ELM and fear appeals to influence privacy and security precautionary behavior have demonstrated desired counter-argumentation results (Wall and Warkentin 2019; Keller and Block 1996). Counter-argumentation occurs when an individual reviews internally available information together with persuasive cues and determines the extent to which these cues influence his or her belief. Similarly, we assert that adopting a similar approach using fear appeals (high and low) with ELM (objective and imagery processing) should have an influence on consumer privacy fatalism.

Integrating fear appeals and elaboration routes with privacy fatalistic beliefs

Fatalistic beliefs have been found to be positively associated with lower intentions to change behavior often leading to negative health outcomes. As such, it is highly probable that reducing or eliminating fatalistic beliefs will consequently encourage behavioral change among fatalistic individuals leading to a reduction in negative health outcomes (Powe & Finnie, 2003). Previous studies have suggested several interventions to help reduce or possibly, eliminate fatalism (McLure et al. 2001; Chomsky 1975 and Siegel 1988). For instance, McLure et al. (2001) explain that people often believe that nothing can be done to reduce damage from earthquakes and other disasters. Such individuals often enter the state of helplessness because their fatalistic beliefs urge them to attribute an earthquake's damage to its magnitude which is an uncontrollable cause rather than attributing the damage to building designs, a fairly controllable cause. McLure et al. found that the attribution of damage to the earthquake magnitude led to less preparation, but the damage attribution to controllable causes such as building design led to more preparations like building regulation compliance and structural strengthening. Therefore, they proposed that public education and news reporting should contain high distinctive and consensus messages. That, these messages should emphasize

the uniqueness of damage from an earthquake and explain how the damage could have been reduced in each distinct event as a way of reducing fatalistic beliefs. Also, Chomsky (1975) and Siegel (1988) encouraged the use of educational programs to reduce fatalistic beliefs. They argued that such programs will create critical-thinking individuals who are likely to resist indoctrination due to high intellectual capability.

We mirror these suggestions by adopting the fear appeal and elaboration likelihood theories. The reason being that fear-appeals literature uses awareness messages as the manipulation mechanism much like the suggestions by McLure et al. (2001) in the preceding paragraph. Milne et al. (2000) states that fear appeal do not present threat warnings only, but also increases the individual's coping efficacy by providing a path to address the potential threat. Thus, fear appeals with both threat and efficacy are effective and recommended in IS literature because they address both the threat and individual's ability to deal with it. This is in accordance with McLure et al.'s suggestion to manipulate individuals to attribute damage causes to controllable causes which can be dealt with. (Milne et al., 2000; Witte & Allen, 2000). Also, the elaboration likelihood allows us to investigate whether critical-thinking is needed to reduce fatalism, in this case, consumer privacy fatalism. This interpretation will be based on which of the routes (objective and imagery processing) form the most effective pair with fear appeals in terms of their impact on consumer privacy fatalism. We believe these two theories are appropriate for the study based on their extensive use in the information security literature.

High fear appeals provoke a higher level of privacy concern compared to low fear appeals. In interventions with high fear appeal messages, individuals will be highly motivated to elaborate on the message due to heightened privacy concerns. This demonstrates a positive relationship between fear appeals and the propensity to elaborate (Keller and Block 1996). We assert that a high fear appeal message will trigger higher levels of privacy concern which should increase an individual's likelihood to elaborate on the message. Therefore, individuals exposed to a high fear appeal message should experience reduced levels of privacy fatalism due to potential message elaboration regardless of the elaboration type (imagery or objective). However, we expect that this reduction in fataslistic beleifs should be stronger at the objective level than the imagery level. This is because when individuals experience heightened privacy concerns, they are more likely to process the argument quality of the fear appeal message. Perceived argument quality has

been found to improve the efficacy of messages delivered in security trainings (Puhakainen and Siponen 2010). Also, higher levels of perceived argument quality have been found to improve individuals' perception of response efficacy (Wall and Warkentin 2019). As such, individuals who process a fear appeal message at the objective level are more likely to believe that they can respond to the threat compared to individuals who process at the imagery level because individuals in the former group are able to recognize the persuasiveness and argument quality of the message than individuals in the latter. Simply put, objective processing tend to have more persuasive influence than imagery processing as individuals who engage in objective processing are able to process the argument quality of the fear appeal message and experience higher perceptions of response efficacy (Cacioppo and Petty 1979; Kisielius and Sternthal 1984). Hence, we postuate that, both imagery and objective processing of high fear appeal messages should lead to reduction in consumer privacy fatalism. However, high fear appeal messages processed at the objective level should have a stronger effect on reducing consumer privacy fatalism compared to those processed at the imagery level.

> Hypothesis 1a: Compared to a control group, individuals who engage in objective processing of a high fear appeal message will demonstrate a reduction in consumer privacy fatalism.
>
> Hypothesis 1b: Compared to a control group, individuals who engage in imagery processing of a high fear appeal message will demonstrate a reduction in consumer privacy fatalism.
>
> Hypothesis 1c: Exposed to a high fear appeal message, individuals who engage in objective processing will demonstrate a greater reduction in consumer privacy fatalism than individuals who engage in imagery processing.

Unlike high fear appeals, low fear appeals do not generate higher levels of privacy concerns. As such, low fear appeals tend to have a limited effect on persuasion because it does not generate sufficient motivation required to elaborate on the message. However, research shows that interventions containing imagery processing can enhance persuasion since they provide individuals with the motivation for message elaboration (Keller and Block, 1996). Under low fear appeals, the challenge is to increase the level of message elaboration and as such, the provision of imagery processing makes it convenient for individuals to elaborate on the message. Imagery processing has been found to be effective at the peripheral route as it

involves low involvement and cognitive effort (Keller and Block, 1996). Therefore, we assert that individuals exposed to interventions with low fear appeals will be less motivated to critically appraise the argument quality of threat and as such, are more likely to resort to mental shortcuts such as imagery processing. Thus, low fear appeal messages targeted at the imagery level should have more impact on persuading fatalistic consumers to respond to threats. Also, we assert that the imagery level has more persuasive influence than the objective level because of counter-argumentation. When a low fear appeal message is processed at the objective level, negative effects of counter-argumentation such as message avoidance or rejection are likely to occur due to lower privacy concerns. Although individuals might still exhibit a reduction in privacy fatalistic beliefs at the objective level, the magnitude of the reduction should be smaller when compared to individuals who engaged in imagery processing.

> Hypothesis 2a: Compared to a control group, individuals who engage in objective processing of a low fear appeal message will demonstrate a reduction in consumer privacy fatalism.
>
> Hypothesis 2b: Compared to a control group, individuals who engage in imagery processing of a low fear appeal message will demonstrate a reduction in consumer privacy fatalism.
>
> Hypothesis 2c: Exposed to a low fear appeal message, individuals who engage in imagery processing will demonstrate a greater reduction in consumer privacy fatalism than individuals who engage in objective processing.

Predicting Likelihood of Opting-in

Privacy schemes and tools exist to provide privacy protection for users. However, they can only serve this function if users opt-in to their usage. Hence, the efficacy of privacy schemes is a function of their adoption and subsequent usage. According to the rational fatalism model, people who believe that the occurrence of future risks is out of their control are more likely to avoid using precautionary measures (Kerwin, 201 2). In relation to privacy issues, users with such beliefs are less likely to adopt privacy schemes to protect their privacy if they believe such attempts are futile and that their personal privacy will still be at risk regardless of whatever schemes they opt-in to. This shows the negative influence of privacy fatalistic beliefs on user attitude toward the adoption of online privacy schemes and tools (OPST). Yao and Daniel (2008) found

that the use of OPST was primarily influenced by an individual's behavioral intentions. Further insights from their study revealed that a favorable attitude toward OPST was a necessary condition for the adoption of these schemes. Therefore, persuasive efforts to motivate the usage of OPST ought to also focus on stimulating a positive attitude from users. Building on the findings from Xie et al., (2019) which state that people with high privacy fatalistic beliefs took fewer steps to protect both informational and social privacy on the internet, we assert that reducing privacy fatalistic beliefs should have a positive influence on users' attitude towards OPST which should then improve their adoption and usage. Simply put, a reduction in a user's level of privacy fatalistic beliefs should increase the likelihood of opting into privacy schemes. This is because users with a positive attitude toward OPST are more likely to opt-into OPST or communicate the intentions to do so (Yao and Daniel, 2008). Although the focal purpose of our study is to introduce an intervening mechanism to reduce consumer privacy fatalism, we assert that users who experience reduced levels of privacy fatalistic beliefs are more likely to communicate an intention to opt-in to OPSTs.

Hypothesis 3: Post-manipulation consumer privacy fatalism will be negatively related to the likelihood of opt-in intention.

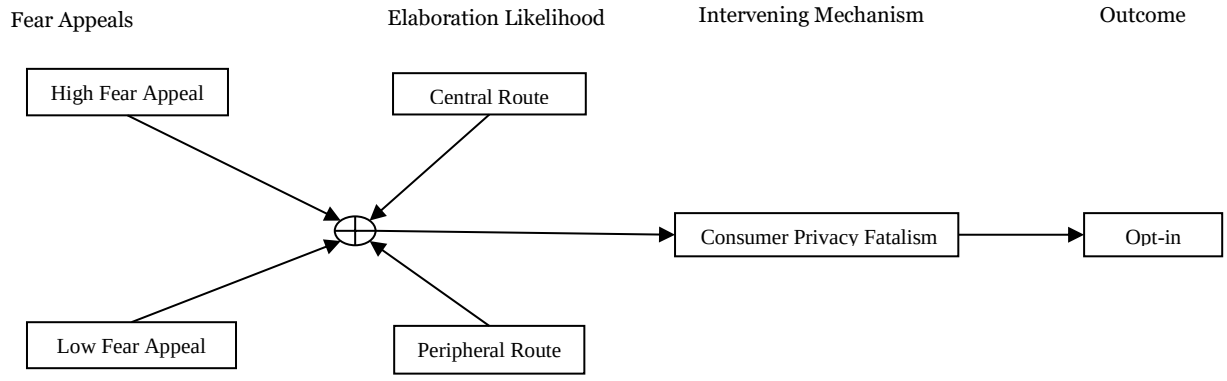

Figure 1: Theoretical Model

Proposed Research Methodology

Research Design

The study will adopt a 2x2 factorial design together with a survey method design to test the proposed hypotheses (Jasso, 2006; Rossi & Anderson, 1982). The factorial survey method is an experimental method

which allows participants to evaluate hypothetical descriptions of objects or scenarios, where attributes are also systemically varied. We expect to develop a survey instrument using hypothetical descriptions of several unique scenarios that contain a subset of the experimental treatments (fear appeals and processing routes). Each scenario should contain language that represents a unique combination of either high/low fear appeal attribute and objective/imagery processing routes. Participants will be presented with surveys containing one unique scenario together with a privacy scheme and asked to answer questions based on their perceptions and the impact these perceptions have on the dependent variable (consumer privacy fatalism and intention to opt-in). Scenario-based methods are often used for behavioral research in information security Herzog, 2003; Seron, Pereira, & Kovath, 2006; Trevino, 1992; Weber, 1992; Johnston et al., 2016; Trinkle, Crossler, & Warkentin, 2014; Willison et al., 2018) because of its simplicity compared to other methods like observation or direct questioning. As such, this study will integrate both the factorial design and scenario-based survey method to ensure all the realistic combinations of all dimensions of each variable being investigated are accounted for and measured using hypothetical scenarios.

To ensure realism, content validity, and face validity, there is the need to convene an expert review panel before distributing the scenario-based survey. This panel should comprise experts in instrumentation and scale development to provide feedback on the generalizability and realism of the scenarios. Feedback from the panel will be used to revise the survey instrument and scenarios to ensure realism and completeness while reducing ambiguity and potential survey fatigue. We then expect to conduct a small pilot study with a convenience sample (mostly undergraduate and graduate students) using the revised survey instrument to confirm discriminant and convergent validity before the actual data collection.

Participants

Participants will be recruited through Mechanical Turk (MTurk), a survey, and an internet panel provided by the Amazon platform. Participants will initially be tested for privacy fatalistic beliefs to ensure that the right sample is used for the study and also, establish a base-line for fatalistic beliefs. This should make it possible to measure post-experimental fatalistic beliefs. The use of M-Turk should also ensure anonymous completion of surveys. To prevent survey fatigue and reduce learning effects, each participant will be

randomly exposed to a version of the survey instrument containing one unique (out of 5 possible) intervention. Also, attention checks will be included in the survey to ensure that survey responses are accurate. Completed survey responses will be subjected to rigorous manipulation checks and quality checks Responses which fail these attention and manipulation checks will be excluded from the final analysis.

Task

The use of MTurk should allow participants to complete the surveys at their own convenience. Participants will be required to read detailed descriptions of scenarios which describes the privacy schemes of a fictional e-commerce platform. The use of an e-commerce platform as the context is supposed to enhance the realism level of the study and make it easier for the participants to relate to the hypothetical scenarios (Appendix). The participants will be presented with privacy schemes from the fictional platform prompting them to opt-in. They will then be required to answer questions on how the schemes affect their fatalistic beliefs and intentions to opt-in.

This study will adapt and modify the scenarios used in Wang et al. (2003). As such, three of the fair information practice principles (FIP) will be embedded in privacy schemes. These FIP principles comprise: the notice/awareness principle, choice/consent principle, and access/participation principle. For the notice/awareness principle, the privacy schemes will provide explicit information for the users to know the type of data being that would be accessed by the platform and how such data will be used. Also, the choice/consent principle will ensure that the schemes provide options for users to control information access. To satisfy the access/participation principle, the schemes will also provide options for users to control who can see their app activities. Additionally, the schemes will provide emphasis on the participants' ability to stop data collection at any point in time, the participants' required approval prior to any data collection activity, and the participants' ability to decide on a granular level the type of data they want to share. The privacy schemes will contain these principles to ensure that they meet the required standards per FIP principles.

Experimental Treatments

To test our hypotheses, we will conduct a 2 (high vs low fear appeal) x 2 (imagery vs objective processing) factorial design. In the high fear appeal treatment, the privacy scheme will request access to highly sensitive information from the participants. Such sensitive information will include participants' names, gender, shopping history, current location, email address, and mailing address. Meanwhile, the low fear appeal treatment will request participants' basic information including name, gender, shopping history. In the imagery treatment, the privacy scheme will be designed using visually descriptive and descriptive language. Under this treatment, we intend to use peripheral cues (visual attractiveness of the schemes) to persuasively stimulate the sensory nodes of the participants. Additionally, participants exposed to the imagery treatment are expected to treat the visual stimuli as a mental shortcut to avoid elaborating on the content of the scheme. However, privacy schemes under the objective treatment will be designed to appeal to the logic of the participants. Special emphasis will be put on crafting the content of the message to enhance its argument quality and persuasiveness. A standard privacy scheme will also be drafted for the control group to serve as a baseline for the hypotheses testing. The inclusion of a baseline is very important since several authors have argued that there are no significant differences between low fear appeals and no fear appeals (Milne et al. 2000). All of the treatments will be tested with a pilot sample and continually revised to produce the desired manipulation effects.

Dependent Variable Measurement

Two variables, consumer privacy fatalism, and intention to opt-in, will be measured as the dependent variables. Participants will initially be tested for privacy fatalistic beliefs to ensure that the right sample is used for the study and also, establish a baseline for fatalistic beliefs. This should make it possible to measure post-experimental fatalistic beliefs. They will then be required to answer questions on the effect of the privacy scheme interventions on their fatalistic beliefs. Since we intend to measure the relationship between privacy fatalistic beliefs and opt-in intentions, respondents will be required to rate their likelihood of opting into the privacy schemes. This should enable us to determine the effect of consumer privacy fatalism as an antecedent to opt-in intentions. To achieve this, this study will conceptually develop a new instrument to measure consumer privacy fatalism as a contribution to the privacy fatalism literature.

Experimental Procedures

Participants will receive a link from MTurk to participate in the study. After completing the initial consent statement, they will be asked to answer filter questions to gauge the level of their privacy fatalistic beliefs. Participants whose belief levels are below the required threshold will not be able to continue the survey. Following the filter questions, participants will be required to read the scenario for the study before they are randomly exposed to one of the privacy schemes. They will be required to answer some manipulation check questions to ensure that their understanding of the scenario is in accordance with the experimental manipulations. Participants will then be randomly exposed to one of the treatments proceeded by questions on the measured variables. Demographic questions will be asked at the end of the survey. Since the study is adopting the factorial survey method, participants will randomly be exposed to 2 treatments. We will limit the number of treatments to two per respondent to reduce survey fatigue and learning effects.

Addressing Potential Bias

The validity and reliability of empirical studies are often affected by various forms of bias including common method bias. To prevent common method bias, it is imperative that certain checks and controls are included in the research process to ensure that the measuring instrument provides an accurate measurement of what it purports to measure. One of such checks can be done through the use of response set questions which should ensure that survey responses that follow a pattern are excluded from the final analysis. Also, we will use manipulation check questions to ensure attention to the response and the desired understanding of the scenarios. Further, there is a need to ensure the realism of the scenarios to produce valid responses. To achieve the desired level of realism, expert panels comprising information system faculty members and doctoral students will be constituted to review the scenarios and questions. Also, a realism question will be included in the survey to control for the effects of scenario realism (Siponen & Vance, 2010).

Potential Contribution

Theoretical Contribution

According to Floyd et al. (2000), threat and the associated fear can be used to persuade individuals to engage in adaptive behavior. The objective of this study is to determine the synergistic effects of fear appeals and elaboration interventions on privacy fatalistic beliefs and opt-in intentions. We anticipate empirical

support for all the hypotheses. First, we expect high fear appeal manipulations to have a greater reduction effect on privacy fatalistic beliefs than low fear appeal manipulations. Compared to low fear appeals, high fear appeals are designed to produce more fear and inspire protection motivation. Therefore, it is logical to expect high fear appeals to have greater persuasion effects on individual fatalistic beliefs. Also, we expect the objective processing in the high fear appeals to have an even greater impact on reducing privacy fatalistic beliefs than imagery processing. However, we expect the reverse to happen in the low fear appeal due to individuals' lower levels of motivation and privacy concerns to objectively process a low fear appeal message.

To be able to measure privacy fatalism, we will conceptually develop and operationalize "consumer privacy fatalism", which will also double as a theoretical contribution to this paper. Also, this study will contribute to the literature on fear appeals and ELM. Specifically, it will provide empirical evidence for the persuasiveness of both theories to reducing consumer privacy fatalism. Previous studies have looked at the impact of both theories on precautionary behaviors and disclosure intentions (Wall and Warkentin 2019; Keller and Block 1996. This study will build on the foundations laid by these studies and examine the impact the fear appeals, and elaboration routes have on consumer privacy fatalism. Xie et al. (2019) used secondary data to measure consumer privacy fatalism. This study will use primary survey data for which there is no existing instrument for consumer privacy fatalism. Therefore, this study provides the opportunity to either adapt one from previous research in other disciplines and contexts. It can also be the platform for consumer privacy fatalism to be conceptually developed and operationalized into a measurable scale. Moreover, findings from this study will add to the debate on whether low fear appeals are equally inefficacy as no fear appeals. By adding a control group, the research design allows us to test for the effect difference between no fear appeals and low fear appeals.

Practical Implications

It is imperative to consider privacy fatalism when designing privacy and security interventions as the efficacy of any intervention depends on its application. If end-users do not believe that the intervention is necessary or effective, then the intervention will fail. Therefore, we expect the findings from this research to provide practical insights to security providers and companies when designing privacy and security interventions. Also, Greg (2019) warns that privacy fatalists may be reluctant to disclose personal data, sign

up for newsletters, offers, or loyalty if these activities mean giving up their privacy. These actions could reduce the effectiveness of such promotional channels. Therefore, privacy fatalists should be inspired to believe that it is still possible to control individual privacy and still engage in online activities.

Appendix: SCENARIO

You are a frequent customer of E-Shop, an online retailer which competes with companies like Amazon and E-Bay. After one purchase session, E-Shop presents you with a privacy scheme with an option to either opt-in or opt-out. This privacy scheme contains a simplified version of the company's privacy policy and a request to access your personal information for secondary purposes like personalization (customized shopping preferences/ targeted ads and efficient customer service). As a customer, you are expected to look at the privacy scheme and make a decision as to either opt-in or out of the scheme.

References:

Beltrán, E.D., Ostrow, D.G. and Joseph, J.G., 1993. Predictors of sexual behavior change among men requesting their HIV-1 antibody status: The Chicago MACS/CCS cohort of homosexual/bisexual men, 1985–1986. *AIDS Education and Prevention*.

Boss, S.R., Kirsch, L.J., Angermeier, I., Shingler, R.A. and Boss, R.W., 2009. If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. *European Journal of Information Systems*, 18(2), pp.151-164.

Cacioppo, J.T. and Petty, R.E., 1979. Effects of message repetition and position on cognitive response, recall, and persuasion. *Journal of personality and Social Psychology*, 37(1), p.97.

Chomsky, N. 1975. "Towards a humanistic conception of education", in Feinberg, W. and Rosemont, H. Jr (Eds), Work, Technology, and Education, University of Illinois Press, Urbana, IL, pp. 204-220.

Clarke, J.H., MacPherson, B.V. and Holmes, D.R., 1982. Cigarette smoking and external locus of control among young adolescents. *Journal of Health and Social Behavior*, pp.253-259.

Correia, J. and Compeau, D., 2017, January. Information privacy awareness (IPA): a review of the use, definition and measurement of IPA. In Proceedings of the 50th Hawaii International Conference on System Sciences.

Culnan, M.J. and Armstrong, P.K., 1999. Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization science*, 10(1), pp.104-115.

Debatin, B., Lovejoy, J.P., Horn, A.K. and Hughes, B.N., 2009. Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of computer-mediated communication*, 15(1), pp.83-108.

Dunfee, T.W., Smith, N.C. and Ross Jr, W.T., 1999. Social contracts and marketing ethics. *Journal of marketing*, 63(3), pp.14-32.

Ermakova, Y.G., Bilan, D.S., Matlashov, M.E., Mishina, N.M., Markvicheva, K.N., Subach, O.M., Subach, F.V., Bogeski, I., Hoth, M., Enikolopov, G. and Belousov, V.V., 2014. Red fluorescent genetically encoded indicator for intracellular hydrogen peroxide. *Nature communications*, 5(1), pp.1-9.

Esparza, O.A., Wiebe, J.S. and Quiñones, J., 2015. Simultaneous development of a multidimensional fatalism measure in English and Spanish. *Current Psychology*, 34(4), pp.597-612.

Fishbein, M., leek Ajzen., 1975. Belief, attitude, intention and behavior: An introduction to theory and research, pp.181-202.

Floyd, D.L., Prentice-Dunn, S. and Rogers, R.W., 2000. A meta-analysis of research on protection motivation theory. *Journal of applied social psychology*, *30*(2), pp.407-429.

Franklin, M.D., Schlundt, D.G., McClellan, L.H., Kinebrew, T., Sheats, J., Belue, R., Brown, A., Smikes, D., Patel, K. and Hargreaves, M., 2007. Religious fatalism and its association with health behaviors and outcomes. *American journal of health behavior*, 31(6), pp.563-572.

Furnell, S. and Clarke, N., 2012. Power to the people? The evolving recognition of human aspects of security. *computers & security*, 31(8), pp.983-988.

Govani, T. and Pashley, H., 2005. Student awareness of the privacy implications when using Facebook. Unpublished paper presented at the "Privacy poster fair" at the Carnegie Mellon university school of library and information science, 9, pp.1-17.

Greg S. 2019. Most consumers believe online privacy is impossible, survey finds. [online] Available at: https://marketingland.com/most-consumers-believe-online-privacy-is-impossible-survey-finds-263538 [Accessed 5 May 2020].

Gregg, J. and Curry, R.H., 1994. Explanatory models for cancer among African-American women at two Atlanta neighborhood health centers: the implications for a cancer screening program. *Social science & medicine,* 39(4), pp.519-526.

Guthrie, L.C., Butler, S.C., Lessl, K., Ochi, O. and Ward, M.M., 2014. Time perspective and exercise, obesity, and smoking: Moderation of associations by age. *American Journal of Health Promotion*, 29(1), pp.9-16.

Herath, T. and Rao, H.R., 2009. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, 47(2), pp.154-165.

Jansen, J. and van Schaik, P., 2019. The design and evaluation of a theory-based intervention to promote security behaviour against phishing. *International Journal of Human-Computer Studies*, 123, pp.40-55.

Johnston, A.C. and Warkentin, M., 2010. Fear appeals and information security behaviors: an empirical study. *MIS quarterly*, pp.549-566.

Johnston, A.C., Warkentin, M. and Siponen, M., 2015. An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS quarterly*, 39(1), pp.113-134.

Joiner Jr, T.E., Perez, M., Wagner, K.D., Berenson, A. and Marquina, G.S., 2001. On fatalism, pessimism, and depressive symptoms among Mexican-American and other adolescents attending an obstetrics-gynecology clinic. *Behaviour research and therapy*, 39(8), pp.887-896.

Karjalainen, M. and Siponen, M., 2011. Toward a new meta-theory for designing information systems (IS) security training approaches. *Journal of the Association for Information Systems*, 12(8), p.3.

Kerwin, J.T., 2012, March. 'Rational fatalism': non-monotonic choices in response to risks. In Working Group in African Political Economy meeting, University of California, Berkeley, CA.

Keller, P.A. and Block, L.G., 1996. Increasing the persuasiveness of fear appeals: The effect of arousal and elaboration. *Journal of consumer research*, 22(4), pp.448-459.

Kirlappos, I., Sasse, M.A. and Harvey, N., 2012, June. Why trust seals don't work: A study of user perceptions and behavior. In International Conference on Trust and Trustworthy Computing (pp. 308-324). Springer, Berlin, Heidelberg.

Kisielius, J. and Sternthal, B., 1984. Detecting and explaining vividness effects in attitudinal judgments. *Journal of marketing research*, 21(1), pp.54-64.

Lee, H., Park, H. and Kim, J., 2013. Why do people share their context information on Social Network Services? A qualitative study and an experimental study on users' behavior of balancing perceived benefit and risk. *International Journal of Human-Computer Studies*, 71(9), pp.862-877.

McClure, J., Allen, M.W. and Walkey, F., 2001. Countering fatalism: Causal information in news reports affects judgments about earthquake damage. *Basic and applied social psychology*, 23(2), pp.109-121.

Michie, S., Van Stralen, M.M. and West, R., 2011. The behaviour change wheel: a new method for characterising and designing behaviour change interventions. *Implementation science*, 6(1), p.42.

Milne, S., Sheeran, P. and Orbell, S., 2000. Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory. *Journal of Applied Social Psychology*, 30(1), pp.106-143.

Neff, J.A. and Hoppe, S.K., 1993. Race/ethnicity, acculturation, and psychological distress: Fatalism and religiosity as cultural resources. *Journal of Community Psychology*, 21(1), pp.3-20.

Oetzel, M.C. and Gonja, T., 2011. The online privacy paradox: a social representations perspective. *In CHI'11 Extended Abstracts on Human Factors in Computing Systems* (pp. 2107-2112).

Phelps, J., Nowak, G. and Ferrell, E., 2000. Privacy concerns and consumer willingness to provide personal information. *Journal of public policy & marketing*, 19(1), pp.27-41.

Posey, C., Roberts, T.L. and Lowry, P.B., 2015. The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems*, 32(4), pp.179-214.

Pötzsch, S., 2008, September. Privacy awareness: A means to solve the privacy paradox?. In IFIP Summer School on the Future of Identity in the Information Society (pp. 226-236). Springer, Berlin, Heidelberg.

Powe, B.D. and Johnson, A., 1995. Fatalism as a barrier to cancer screening among African-Americans: Philosophical perspectives. *Journal of Religion and Health*, 34(2), pp.119-126.

Powe, B.D. and Finnie, R., 2003. Cancer fatalism: the state of the science. *Cancer nursing*, 26(6), pp.454-467.

Puhakainen, P. and Siponen, M., 2010. Improving employees' compliance through information systems security training: an action research study. *MIS quarterly*, pp.757-778.

Roberts, R.E., Roberts, C.R. and Chen, I.G., 2000. Fatalism and risk of adolescent depression. *Psychiatry*, 63(3), pp.239-252.

Rule, J.B., 2007. Privacy in peril: How we are sacrificing a fundamental right in exchange for security and convenience. Oxford University Press.

Scheier, M.F. and Bridges, M.W., 1995. Person variables and health: Personality predispositions and acute psychological states as shared determinants for disease. Psychosomatic medicine, 57(3), pp.255-268.

Shen, L., Condit, C.M. and Wright, L., 2009. The psychometric property and validation of a fatalism scale. *Psychology and Health*, 24(5), pp.597-613.

Sheung-hung, K.T. and Wai-loon, H.C. eds., 2013. Genetic Privacy: An Evaluation Of The Ethical And Legal Landscape. World Scientific.

Siegel, H. 1988. Educating Reason: Rationality, Critical Thinking, and Education, Routledge, New York, NY.

Stutzman, F., Vitak, J., Ellison, N.B., Gray, R. and Lampe, C., 2012, May. Privacy in interaction: Exploring disclosure and social capital in Facebook. In Sixth international AAAI conference on weblogs and social media.

Wade, T., 1996. An examination of locus of control/fatalism for Blacks, Whites, boys, and girls over a two-year period of adolescence. *Social Behavior and Personality: an international journal*, 24(3), pp.239-247.

Wall, J.D. and Buche, M.W., 2017. To Fear or Not to Fear? A Critical Review and Analysis of Fear Appeals in the Information Security Context. *CAIS,* 41, p.13.

Wall, J.D. and Warkentin, M., 2019. Perceived argument quality's effect on threat and coping appraisals in fear appeals: An experiment and exploration of realism check heuristics. *Information & Management*, 56(8), p.103157.

Wang, N., Grossklags, J., & Xu, H. (2013, February). An online experiment of privacy authorization dialogues for social applications. In Proceedings of the 2013 conference on Computer supported cooperative work (pp. 261-272).

Witte, K. and Allen, M., 2000. A meta-analysis of fear appeals: Implications for effective public health campaigns. *Health education & behavior*, 27(5), pp.591-615.

Xie, W., Fowler-Dawson, A. and Tvauri, A., 2019. Revealing the relationship between rational fatalism and the online privacy paradox. *Behaviour & Information Technology*, 38(7), pp.742-759.

Zafeiropoulou, A.M., Millard, D.E., Webber, C. and O'Hara, K., 2013, May. Unpicking the privacy paradox: can structuration theory help to explain location-based privacy decisions?. In Proceedings of the 5th Annual ACM Web Science Conference (pp. 463-472).