



Journal of Information Technology Management

ISSN #1042-1319

A Publication of the Association of Management

UNDERSTANDING ONLINE PRIVACY PROTECTION BEHAVIOR OF THE OLDER ADULTS: AN EMPIRICAL INVESTIGATION

BABITA GUPTA

CALIFORNIA STATE UNIVERSITY MONTEREY BAY

bgupta@csumb.edu

ANITHA CHENNAMANENI

TEXAS A & M UNIVERSITY CENTRAL TEXAS

anitha.chennamaneni@tamuct.edu

ABSTRACT

Study of digital privacy concerns and behavior of older adults is still in nascent stages. This empirical study investigates the antecedents of privacy concerns and the privacy protection behavior of the older adults, and the moderating effect of the potential benefits of digital interactions on their online privacy protection behavior. Our research model is drawn from the Theory of Reasoned Action. Data was collected from 214 older adults and analyzed using PLS structural modeling. The results suggest that the older adults' privacy concerns of engaging in online interactions are significantly affected by the extent of their prior digital usage experience and prior exposure to vulnerabilities related to online fraud. Privacy protection behavior is significantly affected by the privacy concerns. Additionally, our model explores the potential benefits of online use as an antecedent of privacy protection behavior. Potential benefits significantly moderate the effect of privacy concerns on the privacy protection behavior of the older adults. This study contributes to the body of online privacy research and to the study of the digital behavior of the older adults by providing a richer understanding of their privacy protection behavior. The study also provides recommendations to address older adults' fears and vulnerabilities.

Keywords: older adults, privacy concerns, privacy protection behavior, potential benefits, PLS structural modeling

INTRODUCTION

Consumers from all strata of society are increasingly participating in online interactions as a means of communicating and conducting transactions. The proliferation of online interactions is accompanied by a rise in identity thefts, e-mail phishing, spam, spyware, and other Internet fraud mechanisms that can have serious social and economic consequences. Consumers' concerns about loss of their information privacy and ability of an online business to secure their personal information could shape their beliefs and attitudes towards engaging in online communication and transactions. The 2016 Internet

Crime Report¹ highlights that in 2016 Federal Bureau of Investigation (FBI) in the U.S. received 298,728 online fraud complaints with losses exceeding USD 1.3 billion. Older adults of age 50 or higher made up about 39.1% of these online fraud victims in the U.S. population, reporting about 56.6% of losses.

While there are many recent studies about the privacy concerns of consumers as they engage in online activities [35], studies that focus on how the consumers' privacy concerns translate into behavior they adopt to protect their online privacy are still limited [6]. In

¹ https://pdf.ic3.gov/2016_IC3Report.pdf

particular, segment of the older adult population and their privacy protection behaviors are not sufficiently studied. There is very little, to our knowledge, literature that focuses on the digital privacy concerns and privacy protection behavior of older adults. Our study contributes to this nascent body of research by empirically exploring the privacy concerns and behavior of older adults in the context of their online interactions.

We draw upon the Theory of Reasoned Action to develop a theoretical framework for our research model. The research model focuses on the antecedents that shape older adults' privacy concerns regarding sharing their information online; how do their privacy concerns affect their online privacy protection behavior, and what moderating factors might mitigate the relationship between their privacy concerns and the privacy protection behavior.

The paper is organized as follows: next section provides the current literature review of the older adult consumers, their internet use, and the Theory of Reasoned Action (TRA). We then present the research model based on TRA and the research hypothesis. Following that, we describe the research methodology and the data collection methods. Next, we present the empirical data analysis using the structured equation modeling techniques and the results. The following section discusses the findings in the context of the research questions. We conclude the paper with the contributions and managerial implications of this research work followed by the limitations and the future research directions.

LITERATURE REVIEW

Older Adults

The term "older adults" in literature has generally referred to the population of adults in the age range of 40 and above and in the specific labor market context, the term refers to the population of adults aged 50 and above [57], [60].

Over the last few decades, the average life expectancy of the general population has been increasing steadily globally. In this era of rising longevity, most information system research has focused on the internet use of the younger population. Thus, most companies and service providers do not fully understand how the older demographic interacts with the internet and communication technologies.

In the U.S., 14.5% of the population, about 46.18 million people, are 65 years or older [55]. The number of seniors is projected to reach 98.2 million by 2060 [54]. According to the 2014 Pew Research Center report, 59% of seniors report they go online compared to 86% of all

adults, and 47% of seniors say they have a high-speed broadband connection at home [51]. In addition, 77% of older adults have a cell phone. However, the internet use and the broadband adoption rate each drop off dramatically around age 75 [51]. A more recent 2015 report from Pew Research Center identifies that about 39% of adults ages 65 and older do not use the internet, compared with only 3% of 18-29 years old who do not use the internet [1]. Overall, even though a greater number of older adults are online than before, the rate of online participation is slower compared to the younger adults [39].

Older Adults and the Internet Use

Studies suggest that Internet use can have a positive impact on the well-being of older adults reducing depression categorization in this group by 20-28% [10], [26]. Older adults are integrating digital technologies into their everyday lives to check health & medical information, news, play games, book a vacation, invest, pay bills, and check email as well as be able to keep in touch with friends and family [24], [39], [45]. Issues that are a barrier to online use by seniors are the potential threats with concern for the validity of online information and privacy concerns [53].

The 2015 Internet Crime Complaint Center (IC3) report on Internet Crimes stated that [16]:

- Older adults were the largest group among the victims reporting a loss of more than \$ 100,000 from Internet-related crimes.
- Non-payment/non-delivery, overpayment, and identity theft were the three primary mechanisms of fraudulent contacts.
- The most commonly reported Internet-related scam among senior consumers (60+) involved phishing (21%).

As the Internet use among older adults continues to increase, so does their vulnerability to the internet-related fraud. Statistics and research on the topic are limited.

Theory-based Studies about the Older Adults

Pan and Jordan-Marsh [41] used Technology Acceptance Model (TAM) to study the factors that affect Chinese older adults' decisions to adopt the Internet. Braun [3] studied 124 older adults using the Internet by applying the Technology Acceptance Model (TAM) and found that perceived usefulness, trust in a social networking site, and frequency of internet use were the significant factors that encourage or discourage older adults in using social networking sites.

McCloskey [38] study of 110 older adults' online purchasing behavior using TAM found trust in sharing personal information online to have a significant factor in the online shopping usage. Kirchbuchner, Grosse-Puppenthal, Hastall, Distler, and Kuijper [28] study indicated that loss of privacy through misuse of collected data or lack of security was the biggest fear among the elderly in use of the ambient intelligence systems.

With increasing social media use, researchers are also beginning to study privacy preserving actions of adults of age 55 or more when they use specific social media platform, Facebook [6]. Shankar [50] explored the concept of privacy among elderly in the context of pervasive computing at home. This study concluded that the elderly had difficulty in framing the concept of privacy in relation to data protection as they did not see data as a concrete artifact.

The literature review above shows that while there have been many studies focusing on the older adults' internet related activities, and some studies even focused on their privacy concerns and behavior, there is a gap in understanding the following about the online behavior of the older adults:

- What are the privacy concerns of the older adults and how are these concerns affected by their prior experiences both in using the Internet and having a prior negative online experience?
- How do their privacy concerns affect their privacy protection behavior such as opting-out or providing false information?
- How do the potential benefits of online interactions affect older adults' privacy protection behavior?

The above questions provide the motivation for this research study. This study contributes to the extant literature by providing a deeper understanding of the older adults' online behavior.

In the following section, we present the theoretical framework and the research model for this study, followed by the research methodology.

Theory of Reasoned Action (TRA)

Theory of Reasoned Action (TRA) is a widely used theoretical model for the study of attitudes and their relationship to human behavior [15]. TRA makes the key assumption that human beings are rational and make systematic use of information and consider implications before taking actions. TRA hypothesizes that attitudes of a person towards a behavior is the "evaluative effect of

the individual towards performing that behavior" which in turn is a function of a person's belief that a specific behavior leads to a specific outcome [15].

TRA has been applied to strategy choices in healthcare, psychology, and in social sciences [13]. Additionally, TRA has been used to predict and understand intentions, behaviors and outcomes of online consumer behaviors including using information systems, privacy, trust, and information sharing behavior in electronic commerce transactions [12], [59].

RESEARCH MODEL

TRA [15] provides the foundation and structure to examine our research questions in the context of the older adults' online privacy concerns. Main components in TRA are: External Factors, Beliefs, Subjective Norms, and Behavioral Outcome. TRA works well when applied to behaviors that are under a person's volitional control [15]. In our study, our subjects, the older adults, have complete control over their actions in online interactions and therefore exercise their volitional control. We describe the TRA components of our study in the research model in Figure 1:

- External factors have two constructs: 1) older adults' extent of digital usage experience and 2) their prior vulnerability experience when using the Internet.
- Risk beliefs component of TRA is the privacy concerns of the older adults regarding participating in online interactions.
- The moderating variable is the older adults' perception of the potential benefits of engaging in online interactions.
- Behavior component of TRA is the online privacy protection behavior of the older adults.

In our research model, we do not consider subjective norm component of TRA. Subjective norm (perceived social pressure) is a function of belief about how an individual thinks her peers (or individuals important to her) would approve or disapprove of her online behavior (i.e. would they approve if she decided to opt-out or provide false information based on her concern for a company's privacy policies). In our study, this would not be a relevant as an individual's online actions are not public. In other words, the individual's online actions do not necessarily come under the scrutiny of "important others", and therefore, are largely immune to their approval or disapproval.

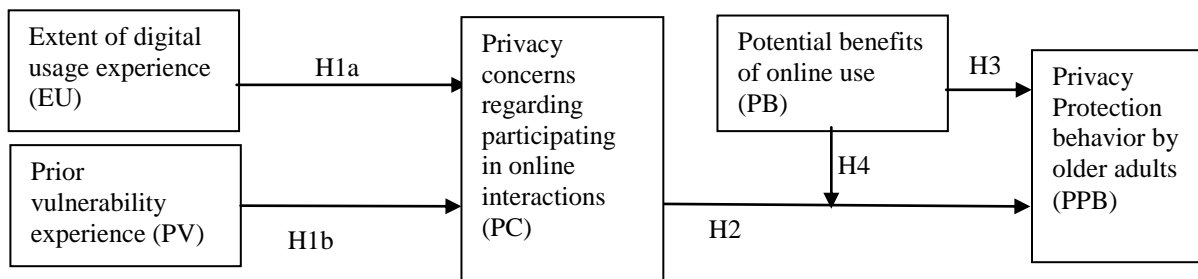


Figure 1: Research Model Using the Theory of Reasoned Action for Older Adults' Online Privacy Protection Behavior

Privacy Concerns (PC)

Concern for Information Privacy (CFIP) by Smith et al. [52] captures an individual's concerns about organizational privacy. CFIP has five dimensions: collection, unauthorized secondary internal use, unauthorized secondary external use, improper access, and errors. This study along with similar studies done in the late 1990s [11] are consistent with the set of online privacy guidelines regarding data collection and use of information developed by the Federal Trade Commission (FTC) [17]. Malhotra et al. [37] adapted the CFIP for the Internet context to define Internet User's Information Privacy Concern (IUIPC) using three factors: collection, control, and awareness of privacy practices. A number of studies used Pavlou's [42] study listing risks associated with engaging in e-commerce, including economic risk, personal risk, and privacy risk and how it is related to CFIP [56].

The type of information being disclosed or shared shapes consumers' online information privacy concerns that in turn shapes their privacy risk belief; and sharing medical and financial information is generally considered more sensitive than sharing lifestyle characteristics, shopping habits and preferences information [25], [30], [32], [43]. Online information privacy concerns arise when a consumer's personally identifiable information is either collected without a consumer's consent or is misused in a manner that is not consistent with FTC's fair information practices of *notice* (consumer is given notice of an entity's information practices); *choice* (consumer has a choice with respect to the use and dissemination of information collected from or about them); *access* (consumer should have access to her information collected and stored by an entity); *security* (data collectors take appropriate steps to ensure the security and integrity of the consumer information

collected); and *redress* (enforcement mechanisms available to consumer to ensure compliance to privacy principles) [19].

Consumers may be guarded in sharing personal, identifying, and sensitive information with firms that may not be adhering to FTC's five core principles [19]. Thus, a consumer's online privacy concerns reflect the potential privacy risks beliefs of consumers [5], [20], [27].

A more detailed review of consumer's information privacy research and the dominant themes in the consumer privacy literature from 1989 to 2007 is found in Lanier and Saini [30].

Privacy literature has drawn a distinction between general privacy concerns and situation specific privacy concerns [34]. In this study, we focus on the situation-specific privacy concerns of the older adults that are based on their beliefs in the company's respect for consumer privacy based on FTC's the five core privacy principles [9].

Our study emphasizes understanding the contextual factors that affect older adults' privacy beliefs and subsequent implications for their willingness to engage in behavior that protects their online privacy. We use privacy concern as the belief construct. Privacy concern construct includes items such as "Company website clearly states how my personal information is collected and used" and "Company website allows me to delete or edit my personal information anytime I want to". Studies have found a positive relationship between consumers' perceptions of a company's respect for consumer privacy (such as websites with strong privacy policies) and consumers' willingness to engage with that company, thus affecting consumers' online behavior such as providing sensitive information or refusing to purchase [31], [36].

External Factors

According to TRA, external factors play an important role in the formation of beliefs. We consider two external factors as the antecedents to older adults' privacy concerns regarding participating in online interactions: 1) older adults' extent of digital usage experience; 2) any prior vulnerability they might have experienced such as having their identity stolen or experienced online fraudulent transactions.

The Extent of Digital Usage Experience (EU)

An older adult's prior experience of digital use is an important factor in the formation of usage beliefs. Older adults who have direct experience with computers tend to display a more positive attitude towards technology use [18]. Prior studies used several factors such as experience with the Internet use, frequency of use, and purpose of the Internet use as indicators of prior online experience [4], [48]. More online experience may lead to lower level of risk aversion to digital use among the older adults [46]. To capture the extent of digital usage experience, and its effect on the older adults' privacy concerns, we propose the following hypothesis:

H1a: The higher extent of prior digital usage experience reduces older adults' privacy concerns regarding participating in online interactions.

Prior Vulnerability Experience (PV)

Prior vulnerabilities can include invasion of privacy, exposure or attacks by viruses, spyware, malware, and/or being a victim of spam and identity thefts [2], [4]. Lee [33] found that consumers' perceived risks of the security/privacy risk (fraud, hacking, phishing, identity theft, loss of control) and financial risk negatively affect the intention to use online banking while the perceived benefit, attitude and perceived usefulness positively affect the intention to use online banking.

Smith, Milberg, and Burke [52] found that privacy invasion experiences as an antecedent had a significant relationship to individual's privacy concerns. Individuals with prior vulnerable experiences with personal information abuses have stronger concerns regarding an organization's information collection and information use practices [37], [43].

Web-based survey of 1005 Internet users showed that consumers are most concerned about data transfer, notice/awareness and storage aspects of fair information practice principals and that prior experience affects their online information sharing practices [14]. Brown and Muchira [4] studied younger students from Australia and found prior privacy invasion experience negatively affected their online purchase behavior.

In this study, we test if prior online vulnerabilities negatively influence older adults' privacy concerns towards online interactions. Thus, we hypothesize the following:

H1b: The higher extent of prior vulnerability experiences increase older adults' privacy concerns regarding participating in online interactions.

Privacy Protection Behavior (PPB)

We examine if the older adults' privacy concerns about engaging in online interactions will result in behavior to protect their personal information. Yao [58] proposed a behavioral approach using the theory of planned behavior to study the self-protective behavior of people to protect their online privacy. The measures for this behavior are consistent with the measures explored by Phelps et al. [43] and Malhotra et al. [37]. They proposed behaviors such as carefully reading privacy statements, managing cookies, opt-out, providing false information, and other precautionary measures. We consider how the older adults' privacy concerns affect their online privacy protection behavior and hence the following hypothesis:

H2: Higher privacy concerns of the older adults regarding participating in online interactions lead to greater privacy protection behavior.

Potential Benefits (PB)

The meta-analysis of existing literature of older adults' use of Internet discusses one of the barriers to computer use by the older adults is the lack of perceived benefits [57]. Apart from older adults' beliefs affecting privacy protection behavior, we also examine if potential benefits of online use moderates the effect of privacy concerns on their online behavior where customers may be persuaded to share their personal information based on the rewards or benefits offered by the companies. Heskett, Sasser, and Hart [23] explored the reverse effect, i.e., firms can improve the perceived benefits of services offered by mitigating a customer's perceived privacy risk. However, consumers will not share information unless the risks can be controlled or eased. Using secondary data from 1998, Awad and Krishnan [2] found that consumers value personalized service more than personalized advertising. However, consumers who like more control over their online information are less likely to provide that information in lieu of personalized offering from the firm. Thus, we form the following hypothesis to explore the effect of potential benefits on the online behavior of the older adults:

H3: Higher potential benefits of participating in online interactions lead to lower privacy protection behavior by the older adults.

Potential Benefit (PB) As a Moderating Factor

Several studies have made the case that individuals treat their personal information as a commodity that can be exchanged for the right economic or non-economic benefits, as perceived by the individual [20], [49]. Individuals are more likely to engage in online transactions if they perceive that their privacy risk is low and potential benefits are high [34].

Survey of 243 consumers with previous online buying experience showed that consumers engage in tradeoffs between convenience from online personalization and privacy [7]. This study measured only the intent to use personalization services and not the actual behavior [7]. We explore if the perceived benefits of online interactions will moderate the relationship between older adults' online privacy concerns and their privacy protection behavior and hence the hypothesis:

H4: The influence of older adults' privacy concerns on their privacy protection behavior will be moderated by the potential benefits of participating in the online interactions.

RESEARCH METHODOLOGY

Based on the literature, we propose the theoretical model (see Figure 1) to delve deeper into the privacy concerns of the older adults, how these concerns relate to their behavioral response in terms of privacy protection actions they take. The theoretical constructs and measures are adapted from prior works including Phelps et al. [43], Malhotra et al. [37], Smith et al. [52], and Gupta et al. [19].

The survey is designed to protect individual respondent's identity and all responses are confidential. We conducted a pilot study of the survey in a public library in a city in north California with a focus group of older adults. The feedback provided resulted in some minor adjustments to the language of the survey. The final survey was then administered in various locations in the northern and central California in the U.S. Survey was made available in both the paper- and web-based format to allow for wider distribution and data collection. In our research study, to broaden the scope of participation, surveys were administered to older adults through community centers, city commissions on disabilities and aging, public libraries, and to older employees in non-

profit, hospitality, government, and education sectors. In some instances, surveys were formatted to ensure readability for across age groups (e.g. using large font type).

We collected 214 valid responses from the older adults (paper-based 47% and web-based 53% responses). Gender distribution of survey respondents showed that 56.1% are females, 36.4% are males, and 7.5% declined to state their gender. 55.1% of adults in the sample are in 51 to 65 years age group and 39.3% of older adults are more than 65 years old. In terms of their education levels, older adults in this sample are largely well educated: 28.5% had a bachelor's degree or a technical degree, 28% had master's degree, 15.4% had a doctorate, 21.5% had some years of college, high school, or less, and 6.6% of the sample declined to share their educational background information.

In terms of their current occupation status, 45.3% are either retired or are homemakers, while 47.7% are employed full-time, part-time or are self-employed, rest did not state their occupation. For the household income, 44.4% of the older adults in the sample reported annual household income of up to USD \$75,000 while 36.4% reported annual household income greater than \$75,000. Rest of the older adults in the sample declined to share their income background information.

Analysis of the marital status of the sample indicates that 59.8% of the older adults are married while the rest are either divorced, widowed, or other, and 8.9% reporting as never been married. 2.3% declined to share their marital status. The ethnic background of this group is largely Caucasian (65.9%) with 17.3% identifying as Asian/Pacific Islander with 4.7% identifying in other ethnic categories including African American, Hispanics, and American Indian or Alaska Natives. 12.1% reported their ethnicity as "other" or declined to state it.

The living arrangement of this sample group varied with 26.2% living independently, 0.5% living in the assisted living arrangements, 56.1% living with spouse or partner, 6.5% living in senior retirement homes, and 2.8% living in other arrangements such as living with a family member. 2.3% declined to share their living arrangement background information.

The Internet usage experience profile indicates that the median years of Internet experience is about 10.5 years with only 4.7% of the older adults indicating less than 2 years of the Internet use experience. 78% of these older adults rate themselves as experienced or expert level users of the Internet.

Online shopping profile of this sample indicates that over a period of previous three months from the time of the survey, 22.4% did not buy any items or services online, 55.1% had made 1-6 online purchases, 12.6% had

purchased more than 6 items/services online, and 9.8% did not share this information. In terms of the total dollar (USD) amount spent on online purchases by this sample group, 20.6% had spent a total of \$1 to \$100 in previous three months, 29.9% had spent a total of \$101 to \$500, 8.9% spent a total of \$501 to \$1000, and 6.5% had spent a total amount of more than \$1000 on their online purchases. 23.4% did not spend any amount on online purchases (\$0), and 10.7% chose not to disclose this information.

DATA ANALYSIS & RESULTS

We used Partial Least Squares [8] for testing the research model and to conduct our data analyses. PLS is a component-oriented structural equation modeling technique. It allows for modeling of second-order factors, places minimal demands on sample sizes, and is well suited for both exploratory and confirmatory research. SmartPLS version 3.2.6 [47] was employed to validate the measurement model and to evaluate the overall quality and relationships within the structural model.

Reliability, Validity, and Common Method Variance

We ascertained the adequacy of measurement model by examining the reliability of individual items, internal consistency between items, and by assessing both the convergent and discriminant validities of the model. Table 1 shows average variance extracted (AVE), composite reliability and correlations between the constructs. As shown in Table 1, the composite reliability scores for all constructs exceed the recommended value of 0.80, with most of them being well over 0.90, indicating good internal consistency [40]. AVE scores range from 0.69 to 0.97, exceeding the recommended minimum value of 0.50, thus implying adequate convergent validity.

Discriminant validity was ascertained by ensuring that (i) the square root of the construct's AVE (bold figures on the diagonal in Table 1) is larger than its correlations with other constructs and (ii) the loading for the measurement item on its own construct is higher than its loading on any other unrelated constructs (see Table 1). Table 2 shows that all measurement items exceed the recommended value of 0.7 and load higher on their intended construct than on any other unrelated constructs.

To reduce the risk of common method bias, we employed a number of preventive steps during the design of the survey instrument as recommended by Podsakoff, MacKenzie, Lee, and Podsakoff [44]. We preserved and guaranteed anonymity to the respondents, randomized items on the survey instrument and reverse coded a number of items to increase measurement accuracy. We also conducted post hoc tests and found that common method bias does not pose a serious concern to our interpretation of data.

For post hoc analysis, we performed two tests: Harman's single-factor test using exploratory factor analysis [21], [22] and a full collinearity assessment for all the independent and dependent variables in our model [29]. The results of Harman's single-factor test showed neither the emergence of a single major factor nor any one single general factor account for the majority of the total variance among measures. The items in our dataset loaded on five separate factors, indicating that the common method bias is not a problem. Additionally, the full collinearity test for all the independent and dependent variables in our research model showed that the variance inflation factors (VIF) values for all but one variable were equal to or lower than the most conservative threshold of 3.3 [29]. The highest VIF value is 3.4. Collectively, the results of post hoc tests suggest that common method bias and multicollinearity are not likely a serious concern for our data set.

Table 1: Composite Reliability (CR), Average Variance Extracted (AVE) and Correlation Between Constructs

	CR	AVE	1	2	3	4	5
EU (1)	0.94	0.69	0.83				
PB (2)	0.85	0.75	0.16	0.86			
PV (3)	0.99	0.97	0.11	0.39	0.98		
PPB (4)	0.97	0.86	0.14	0.14	0.69	0.93	
PC (5)	0.97	0.83	0.18	0.08	0.59	0.76	0.91
The diagonal elements (in bold) represent the square root of the AVE							

Table 2: Item Loadings and Cross Loadings

Items	EU	PB	PV	PPB	PC
PB1	0.14	0.93	0.40	0.14	0.08
PB2	0.14	0.79	0.26	0.08	0.05
PC1	0.15	0.02	0.50	0.68	0.93
PC2	0.15	0.03	0.48	0.61	0.91
PC3	0.15	0.06	0.52	0.67	0.95
PC4	0.13	0.06	0.47	0.62	0.91
PC5	0.15	0.05	0.49	0.64	0.93
PC6	0.20	0.11	0.54	0.66	0.92
PC7	0.21	0.15	0.68	0.87	0.80
PPB1	0.14	0.11	0.66	0.97	0.73
PPB2	0.13	0.11	0.64	0.94	0.72
PPB3	0.14	0.16	0.70	0.92	0.73
PPB4	0.14	0.12	0.67	0.93	0.74
PPB5	0.12	0.10	0.63	0.95	0.74
PPB6	0.09	0.18	0.52	0.86	0.58
PV1	0.11	0.41	0.99	0.68	0.59
PV2	0.11	0.41	0.99	0.68	0.59
PV3	0.11	0.39	0.98	0.67	0.59
PV4	0.11	0.35	0.97	0.67	0.56
PV5	0.12	0.38	0.99	0.69	0.58
PV6	0.10	0.38	0.97	0.68	0.57
EU1	0.70	0.10	0.11	0.16	0.18
EU2	0.83	0.17	0.12	0.11	0.13
EU3	0.90	0.17	0.16	0.15	0.18
EU4	0.74	0.04	0.00	0.04	0.12
EU5	0.81	0.08	0.04	0.02	0.07
EU6	0.92	0.16	0.09	0.13	0.18
EU7	0.89	0.16	0.06	0.11	0.12

Structural Model and Hypothesis Testing

The structural model was examined by estimating the path coefficients and R-square values. Figure 2 presents the results for the structural model. The proposed research model has high explanatory power. It explains about 36% of the variance for privacy concerns and 60% of the variance for privacy protection behavior. The results of the hypothesis tests provide strong support for four out of five hypotheses; with two of the five path coefficients statistically significant at 0.01 level, and the other two at 0.05 level respectively (see Figure 2).

As hypothesized, significant relationships were found between prior digital usage experience and privacy concerns (H1a), prior vulnerabilities and privacy concerns (H1b), privacy concerns and privacy protection behaviors (H2). The relationship between potential benefits of online use and the privacy protection behavior was found not to be significant (H3), however, the moderating effect of potential benefits on the relationship between privacy concerns and privacy protection behavior was found to be significant (H4). Table 3 presents the results of the hypothesis testing.

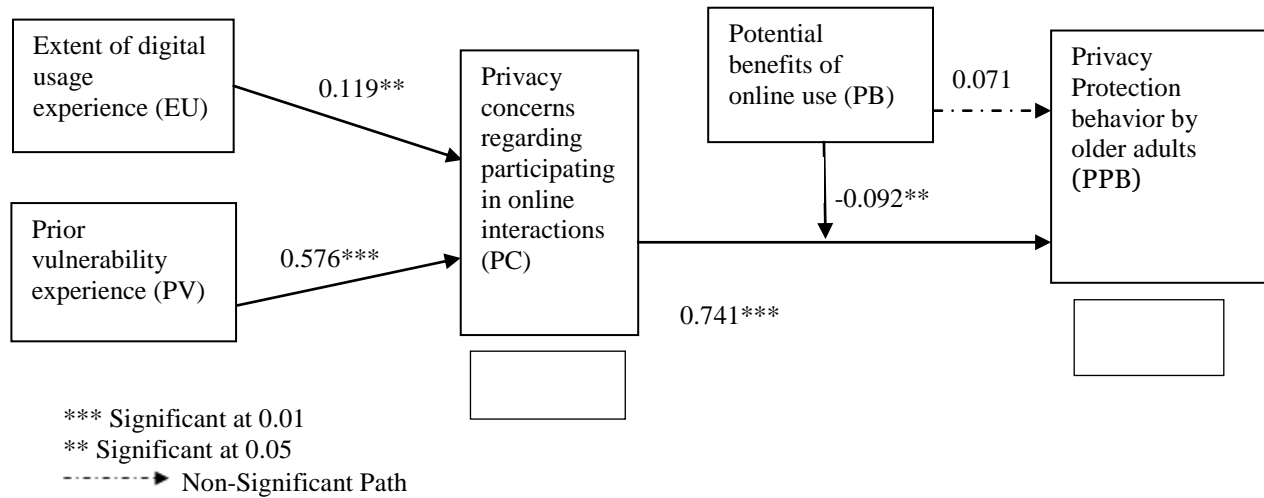


Figure 2: Results of SmartPLS

Table 3: Strength of Paths and T-statistics

	Coefficients	Standard Deviation	T-Statistics	Result
H1a	0.119**	0.056	2.120	Supported
H1b	0.576***	0.066	8.736	Supported
H2	0.741***	0.058	12.867	Supported
H3	0.071*	0.037	1.899	Not Supported
H4	-0.092**	0.043	2.151	Supported

Note: *** Significant at 0.01, ** Significant at 0.05

DISCUSSION

Our study results indicate that the external factors: extent of digital usage experience and prior vulnerability experience related to Internet fraud have a significant effect on older adults’ privacy concerns regarding participating in online interactions. Among the two, exposure to prior vulnerabilities was more significant with a path coefficient of 0.576 followed by the extent of digital usage experience (0.119). These findings agree with previously published research on e-commerce which has indicated that fraud, privacy risks, and financial risks negatively affects individual’s intention to engage in online behaviors [4], [33]. The growing incidence of fraud targeted at older adults is a major concern. Those that have been exposed to fraud find it to be a devastating experience. To protect the older adults from fraud and to reduce their fears and vulnerabilities, it is important to provide educational programs/workshops aimed at older adults’ on strategies to avoid becoming a victim and the redress mechanisms available to them in case they come across a likely fraudulent interaction. Study findings also

indicate that as the extent of digital usage experience increases, older adults’ privacy concerns are lowered. This is consistent with other studies of the general population [4], [46], [48].

Older adults’ privacy concerns regarding participating in online interactions were found to have a significant effect on their privacy protection behavior with a path coefficient of 0.741. This finding is consistent with the prior literature on privacy and Internet use [43], [37]. Older adults’ concern about the loss of privacy can shape their beliefs towards engaging in online privacy protection behavior. To encourage high online usage, online companies should institute measures such as opting-out, managing cookies effectively, and other precautionary measures to lower privacy concerns.

Potential benefits of online use were found not to exert a significant effect on privacy protection behavior with a path coefficient of 0.071. Even as older adults perceive more benefits and convenience of participating in online transactions, their privacy protection behavior remains unchanged. However, the moderating effect of potential benefits on the relationship between privacy

concerns and privacy protection behavior was found to be significant with a path coefficient of -0.092. Higher potential benefits can sway older adults to take less privacy protection measures, even when privacy concerns are higher. This is consistent with prior studies that examined the interaction of online potential benefits and online privacy concerns [7], [34]. Though older adults may perceive high risks in participating in online transactions, companies aiming products at older adults may be able to get higher participation by them if the potential benefits of online use are increased and privacy concerns are lowered.

THEORETICAL CONTRIBUTIONS & IMPLICATIONS FOR PRACTICE

This research work offers several theoretical contributions and managerial implications to the nascent body of literature on the digital privacy concerns and protection behavior of older adults. Additionally, it contributes to the extant literature on the use of TRA in information systems research and information privacy.

Our study findings provide a richer understanding of the older adults' privacy concerns, antecedents of privacy concerns, privacy protection behavior, and the moderating effect of the potential benefits on older adults' online privacy protection behavior. Results from an empirical study of 214 older adults with different demographics, work experiences, education levels, and living arrangements, show that older adults' online privacy concerns are shaped by their prior vulnerability experiences as well as their experience in using digital media. Older adults with prior vulnerable experiences such as fraud, misuse, stolen identity, privacy loss, etc. have a higher level of privacy concerns regarding participating in online interactions. Accordingly, they tend to engage more in privacy protection behaviors such as carefully reading privacy policies, managing cookies, opting out, providing false information, and adopting other precautionary measures while online. However, their engagement in privacy protection behavior could get diluted if a website promises higher potential benefits to them. Potential benefits moderate the relationship between older adults' privacy concerns and their privacy protection behaviors. Higher potential benefits can sway older adults to take less privacy protection measures, even when the privacy concerns are higher. This is a serious concern as companies with weak privacy policies could unduly influence older adults with the promise of higher benefits and overcome older adults' privacy concerns. A more promising strategy to lower the fears, vulnerabilities, and

privacy concerns of older adults would be to offer a high level of privacy protection measures.

Our findings have important managerial implications. Practitioners should design effective privacy measures to protect online information. Companies should clearly inform the older adults about company's privacy and security practices and the controls company have in place so older adults can engage in privacy protection behaviors effectively. They should adhere to FTC's core privacy principles such as displaying privacy policies, third-party privacy seals on their websites etc. Older adults should be informed of how their personal information is being used and if it is shared with other external parties without their consent. Additionally, city and state services can provide informational resources including educational programs and workshops that help protect older adults from online fraud, abuse, and misuse.

LIMITATIONS AND FUTURE RESEARCH

There are few limitations to this study that should be taken into consideration for future research. First, though the posited relationships between the constructs in our research model are grounded in theory and have theoretical support for the direction of the hypothesis, the study findings are based on cross-sectional survey data. The participants in the study are from various locations in the north and central California. Future research will benefit from replicating the study using longitudinal data and from participants across other regions in North America and other countries to provide further support to the relationships. It is also recommended to conduct qualitative interviews to receive the benefits of triangulation.

Second, our study focused on a selected set of research constructs: extent of digital usage experience, prior vulnerability experience, privacy concerns, potential benefits of online use, and privacy protection behaviors. While the research constructs selected in our study are representative of privacy-protection research, they are not exhaustive. Future research may consider other factors that might influence older adults' digital privacy protection behaviors. The moderating effect of older adults' age, occupation, ethnicity etc. should also be investigated.

REFERENCES

- [1] Anderson, M. & Perrin, A. (2016), 13% of Americans don't use the internet. Who are they. *Pew Research Center*, 7. Retrieved October 6, 2017

- from <http://www.pewresearch.org/fact-tank/2016/09/07/some-americans-dont-use-the-internet-who-are-they/>
- [2] Awad, N. F. & Krishnan, M. S. (2006), "The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization", *MIS quarterly*, Vol 30 No. 1, pp. 13-28.
- [3] Braun, M. T. (2013), "Obstacles to social networking website use among older adults", *Computers in Human Behavior*, Vol 29 No. 3, pp. 673-680.
- [4] Brown, M. & Muchira, R. (2004), "Investigating the relationship between Internet privacy concerns and online purchase behavior", *Journal of Electronic Commerce Research*, Vol 5 No. 1, pp. 62-70.
- [5] Castañeda, J. A. & Montoro, F. J. (2007), "The effect of Internet general privacy concern on customer behavior", *Electronic Commerce Research*, Vol 7 No. 2, pp. 117-141.
- [6] Chakraborty, R., Vishik, C. & Rao, H. R. (2013), "Privacy preserving actions of older adults on social media: Exploring the behavior of opting out of information sharing", *Decision Support Systems*, Vol 55 No. 4 pp. 948-956.
- [7] Chellappa, R. K. & Sin, R. G. (2005), "Personalization versus privacy: An empirical examination of the online consumer's dilemma", *Information technology and management*, Vol 6 No. 2-3, pp. 181-202.
- [8] Chin, W. W., Marcolin, B. L. & Newsted, P. R. (2003), "A partial least squares latent variable modeling approach for measuring interaction effects: Results from a Monte Carlo simulation study and an electronic-mail emotion/adoption study", *Information systems research*, Vol 14 No 2, pp. 189-217.
- [9] Commission, U. S. F. T. & Protection, U. S. F. T. C. B. O. C. (1998). *Privacy online: a report to Congress*, US FTC. Retrieved January 3, 2018 from <https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf>.
- [10] Cotten, S. R., Ford, G., Ford, S. & Hale, T. M. (2012), "Internet use and depression among older adults", *Computers in human behavior*, Vol 28 No 2, pp. 496-499.
- [11] Culnan, M. J. & Armstrong, P. K. (1999), "Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation", *Organization science*, Vol 10 No 1, pp. 104-115.
- [12] Doane, A. N., Pearson, M. R. & Kelley, M. L. (2014), "Predictors of cyberbullying perpetration among college students: an application of the theory of reasoned action", *Computers in human behavior*, Vol 36, pp. 154-162.
- [13] Eagly, A. H. & Chaiken, S. (1993), *The psychology of attitudes*, Harcourt Brace Jovanovich College Publishers.
- [14] Earp, J. & Anton, A. (2004), "Addressing end-user privacy concerns", *Proceedings of the Tenth Americas Conference on Information Systems*, New York, 2004
- [15] Fishbein, M. & Ajzen, I. (1975), *Belief, attitude, intention and behavior: An introduction to theory and research*. Reading, MA: Addison-Wesley.
- [16] Federal Bureau of Investigation. 2015. *Internet Crime Report*. Retrieved on January 4, 2018 from https://pdf.ic3.gov/2015_ic3report.pdf.
- [17] Fortes, N. & Rita, P. (2016), "Privacy concerns and online purchasing behaviour: Towards an integrated model", *European Research on Management and Business Economics*, Vol 22 No 3, pp.167-176.
- [18] González, A., Ramírez, M. P. & Viadel, V. (2015), "ICT learning by older adults and their attitudes toward computer use", *Current gerontology and geriatrics research*, 2015.
- [19] Gupta, B., Iyer, I. S. & Weisskirch, R. S. (2010), "Facilitating global e-commerce: A comparison of consumers' willingness to disclose personal information online in the US and in India", *Journal of electronic commerce research*, Vol 11 No 1, pp. 41-53.
- [20] Hann, I.-H., Hui, K.-I., Lee, T. & Png, I. (2002), "Online information privacy: Measuring the cost-benefit trade-off", *Proceedings of the International Conference on Information Systems*, Barcelona, Spain, 2002.
- [21] Harman, H. H. (1967), *Modern factor analysis*., University of Chicago Press.
- [22] Harman, H. H. (1976), *Modern factor analysis*, University of Chicago Press.
- [23] Heskett, J. & Sasser, W. Hart Jr. and CWL . (1990), *Service Breakthroughs: Changing the Rules of the Game*, Free Press, New York.
- [24] Hill, R., Beynon-Davies, P., & Williams, M. D. (2008), "Older people and internet engagement: Acknowledging social moderators of internet adoption, access and use", *Information Technology & People*, Vol 21 No 3, pp. 244-266.
- [25] Huberman, B. A., Adar, E. & Fine, L. R. (2005), "Valuating privacy", *IEEE Security & Privacy*, Vol 3 No 5, pp. 22-25.

- [26] Ihm, J. & Hsieh, Y. P. (2015), "The implications of information and communication technology use for the social well-being of older adults", *Information, Communication & Society*, Vol 18 No 10, pp. 1123-1138.
- [27] Kansal, P. (2014), "Online privacy concerns and consumer reactions: Insights for future strategies", *Journal of Indian Business Research*, Vol 6 No 3, pp.190-212.
- [28] Kirchbuchner, F., Grosse-Puppenthal, T., Hastall, M. R., Distler, M. & Kuijper, A. (2015), "Ambient intelligence from senior citizens' perspectives: Understanding privacy concerns, technology acceptance, and expectations", European Conference on Ambient Intelligence. Springer, pp. 48-59.
- [29] Kock, N. (2015), "Common method bias in PLS-SEM: A full collinearity assessment approach", *International Journal of e-Collaboration (IJeC)*, Vol 11 No 4, pp.1-10.
- [30] Lanier Jr, C. D. & Saini, A. (2008), "Understanding consumer privacy: A review and future directions", *Academy of Marketing Science Review*, Vol 12 No 2, pp.1-48.
- [31] Lauer, T. W. & Deng, X. (2007), "Building online trust through privacy practices", *International Journal of Information Security*, Vol 6 No 5, pp. 323-331.
- [32] Laufer, R. S. & Wolfe, M. (1977), "Privacy as a concept and a social issue: A multidimensional developmental theory", *Journal of social Issues*, Vol 33 No 3, pp. 22-42.
- [33] Lee, M.C. (2009), "Factors influencing the adoption of internet banking: An integration of TAM and TPB with perceived risk and perceived benefit", *Electronic commerce research and applications*, Vol 8 No 3, pp. 130-141.
- [34] Li, H., Sarathy, R. & Xu, H. (2010), "Understanding situational online information disclosure as a privacy calculus", *Journal of Computer Information Systems*, Vol 51 No 1, pp. 62-71.
- [35] Lips, A. M. B. & Eppel, E. A. (2017), "Understanding and explaining online personal information-sharing behaviours of New Zealanders: a new taxonomy", *Information, Communication & Society*, Vol 20 No 3, pp. 428-443.
- [36] 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*, Vol 35 No 4, pp. 572-585.
- [37] Malhotra, N. K., Kim, S. S. & Agarwal, J. (2004), "Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model", *Information systems research*, Vol 15 No 4, pp. 336-355.
- [38] McCloskey, D. W. (2006), "The importance of ease of use, usefulness, and trust to online consumers: An examination of the technology acceptance model with older consumers", *Journal of Organizational and End User Computing*, Vol 18 No 3, pp. 47-65.
- [39] McMurtrey, M. E., Zeltmann, S. M., Downey, J. P. & Mcgaughey, R. E. (2011), "Seniors and technology: Results from a field study", *Journal of Computer Information Systems*, Vol 51 No 4, pp. 22-30.
- [40] Nunnally, J. C. & Bernstein, I. (1994), *Validity. Psychometric theory*, pp. 99-132.
- [41] Pan, S. & Jordan-Marsh, M. (2010), "Internet use intention and adoption among Chinese older adults: From the expanded technology acceptance model perspective", *Computers in human behavior*, Vol 26 No 5, pp. 1111-1119.
- [42] Pavlou, P. A. (2003), "Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model", *International journal of electronic commerce*, Vol 7 No 3, pp. 101-134.
- [43] Phelps, J., Nowak, G. & Ferrell, E. (2000), "Privacy concerns and consumer willingness to provide personal information", *Journal of Public Policy & Marketing*, Vol 19 No 1, pp. 27-41.
- [44] Podsakoff, N. (2003), "Common method biases in behavioral research: A critical review of the literature and recommended remedies", *Journal of Applied Psychology*, Vol 88 No 5, pp. 879-903.
- [45] Quan-Haase, A., Martin, K. & Schreurs, K. (2016), "Interviews with digital seniors: ICT use in the context of everyday life", *Information, Communication & Society*, Vol 19 No 5, pp. 691-707.
- [46] Reisenwitz, T., Iyer, R., Kuhlmeier, D. B. & Eastman, J. K. (2007), "The elderly's internet usage: an updated look", *Journal of Consumer Marketing*, Vol 24 No 7, pp. 406-418.
- [47] Ringle, C. M., Wende, S. & Becker, J.-M. (2015), *SmartPLS 3*. Boenningstedt: SmartPLS GmbH.
- [48] Salam, A. F., Iyer, I., Palvia, P. & Singh, R. (2005), "Trust in e-commerce", *Communications of the ACM*, Vol 48 No 2, pp. 72-77.
- [49] Sayre, S. & Horne, D. (2000), "Trading secrets for savings: How concerned are consumers about club

cards as a privacy threat?", *ACR North American Advances*, Vol 27, pp. 151-155.

- [50] Shankar, K. (2010), "Pervasive computing and an aging populace: methodological challenges for understanding privacy implications", *Journal of Information, Communication and Ethics in Society*, Vol 8 No 3, pp. 236-248.
- [51] Smith, A. (2014), *Older adults and technology use*, Pew Research Center [Internet & American Life Project].
- [52] Smith, H. J., Milberg, S. J. & Burke, S. J. (1996), "Information privacy: measuring individuals' concerns about organizational practices", *MIS quarterly*, Vol 20 No 2, pp. 167-196.
- [53] Tatnall, A. & Lepa, J. (2003), "The Internet, e-commerce and older people: an actor-network approach to researching reasons for adoption and use", *Logistics Information Management*, Vol 16 No 1, pp. 56-63.
- [54] United States Census Bureau. (2014), *National Population Projections Tables*, available at: <https://www.census.gov/data/tables/2014/demo/popproj/2014-summary-tables.html> (accessed on 15 December, 2017).
- [55] United States Census Bureau. (2015), *ACS Demographic and Housing Estimates. 2011-2015 American Community Survey 5-Year Estimates*, available at <https://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml> (accessed on 15 December, 2017).
- [56] Van Slyke, C., Shim, J., Johnson, R. & Jiang, J. J. (2006), "Concern for information privacy and online consumer purchasing", *Journal of the Association for Information Systems*, Vol 7 No 6, pp. 415-444.
- [57] Wagner, N., Hassanein, K. & Head, M. (2010), "Computer use by older adults: A multi-disciplinary review", *Computers in human behavior*, Vol 26, pp. 870-882.
- [58] Yao, M. Z. (2011), "Self-protection of online privacy: A behavioral approach", *Privacy online*. Springer. pp.111-125.
- [59] Yousafzai, S. Y., Foxall, G. R. & Pallister, J. G. (2010), "Explaining internet banking behavior: Theory of reasoned action, theory of planned behavior, or technology acceptance model?", *Journal of applied social psychology*, Vol 40 No 5, pp. 1172-1202.
- [60] Yu, r. P., Ellison, N. B., Mccammon, R. J. & Langa, K. M. (2016), "Mapping the two levels of digital divide: Internet access and social network site adoption among older adults in the USA",

Information, Communication & Society, Vol 19 No 10, pp. 1445-1464.

AUTHOR BIOGRAPHIES

Anitha Chennamaneni is Chair and Associate Professor of the Computer Information Systems in the College of Business Administration at Texas A&M University - Central Texas. Her research interests include cybersecurity, information privacy, big data analytics, knowledge management, and social networking technologies.

Babita Gupta is a Professor of Information Systems in the College of Business at California State University Monterey Bay. Her research interests include data analytics, information privacy and security, organization culture, and the role of gender and power in IS.