Knowledge of Online Security Risks and Consumer Decision Making: An Experimental Study

Ping An Wang
Graduate School of Computer and Information Sciences
Nova Southeastern University
pingan@nova.edu

Easwar Nyshadham
Graduate School of Computer and Information Sciences
Nova Southeastern University
easwar_nash@yahoo.com

Abstract

When the precise risk probability or consequence is not known, as is the case with many online security risks, it is not clear how people judge and respond to such risks. In this research, we study the impact of e-commerce consumers' knowledge of online security risks on their risk evaluation and purchase intentions. Based on research in the decision theory field, we categorize a person's knowledge of a risk as falling under one of four states: known certainty, known uncertainty, unknown uncertainty, and unknowable uncertainty. Following a pilot experiment to test and refine the experimental design, a between-subject experiment is conducted with the four knowledge states as treatments among 160 subjects. Results suggest that willingness to pay and intention to purchase vary systematically under different knowledge conditions. Statistical analysis of the results provides further support for the research model and hypotheses.

1. Introduction

While consumers of B2C (business-to-consumer) e-commerce benefit from fast-growing Internet usage and online shopping activities, they also face increasing online security risks, such as identity theft, credit card fraud, and spyware [27]. Considerable research has discussed consumer decision making in B2C context given the widespread and novel risks [4, 9, 18, 32, 44]. Typically, the existing research assumes that consumers judge i) the subjective probability of a loss, and, ii) the subjective magnitude of consequences of the loss, and compute an expectation of loss. Existing studies primarily focus on determinants of subjective probability and value [25, 31, 36, 48] and the effects of context variables on decision making [40, 41, 45, 47].

An important problem is that neither the probability of occurrence of online risks nor the consequences of risky events are always known to consumers. For example, the likelihood and consequences of a credit card fraud or identity theft resulting from an online transaction are not known for sure even to experts [2, 30, 34]. Thus, the question arises as to how consumers judge and evaluate online risks in the absence of information necessary to judge risks.

For instance, consider a rather familiar scenario in which a consumer is trying to decide whether to engage in an online transaction. She is concerned about (say) the likelihood of identity theft resulting from the transaction but has no reliable data to decide whether it is worth transacting given the risk. She finds that online firm A offers a 100% guarantee for all transactions, thus making an uncertain situation a certain one. Firm B offers a realistic picture of the risk situation (by saying that there is a small but non-zero percent chance of risk); however, for a small additional payment, the firm takes all responsibility should that incident occur.

Firm C says that the risk probability is not precisely known but is no higher than (say) x% and offers an option for consumer to pay a premium to avoid risk. Finally, Firm D suggests that, due to the enormous difficulties in collecting data as well as concerns about accuracy of reporting by victims, it is really impossible to know what the risk is and no one has figured out a reliable way of estimating the risk.

In this paper, we suggest that the four scenarios discussed above represent different notions of uncertainty. A decision maker, in general, can view a decision situation as one involving one of the variants of uncertainty implicit in the above examples. The attitudes and behaviors of the decision maker will be strongly influenced by the assumption they make about the nature or variant of uncertainty inherent in the decision task.

The purpose of this research is to propose and test a preliminary model incorporating the fine-grained distinctions of uncertainty. In Section 2, we review the terminology and literature on decision under uncertainty in general, with focus on decisions in the information systems (IS) domain. Section 3 discusses the research model and generates hypotheses. Section 4 discusses the design of an experiment, instruments, and data collection procedures. Data analysis and interpretation are reported in Section 5, and Section 6 concludes the paper.

2. Literature review

2.1. Terminology and definitions

The terms risk and uncertainty have different meanings across disciplines. We discuss and illustrate these terms using concepts from decision theory. Consider an urn which has a collection of balls of different colors. If a decision maker knows that there are 10 balls and all are blue, it is a case of *certainty*. If the urn is known to have 10 balls and 5 are red and 5 are blue, in a particular draw a decision maker can draw a blue or a red ball. One might arrive at the conclusion that 50% balls are blue using a long-run frequency or frequentist or a subjective/Bayesian interpretation. This case of "known probabilities" is covered under *decision making under risk* in standard texts and is well known in literature [3, 5, 20].

Following Hogarth and Kunreuther [22], suppose the decision maker does not know the proportion of the ball color in a lot of 10 in an urn. A judgment on the likelihood of a red ball in a draw depends on prior knowledge of the distribution of red (R) and blue (B) balls in the urn. A decision maker can start by constructing a "second order" probability distribution about the proportion of balls in the urn across the 11 cases - for example, {0R, 10B}, {1R, 9B}, ..., {10R, 0B}. To judge whether a ball drawn at random from the urn is blue, a decision maker then uses a particular second order distribution from the 11 possible cases. If the second order distribution is not known, then it is a case of *uncertainty*.

Two special cases arise under uncertainty. If a subject cannot eliminate any of the 11 possible cases, then the situation falls under *ignorance* [22] – a special case of uncertainty. On the other hand, if the subject can simplify the problem by eliminating some of the cases (e.g., the number of red balls is known to be always even), he can reduce the number of possible second order distributions - this is a special case of uncertainty called *ambiguity* [3, 11].

In summary, decisions can be made under certainty, risk (known probabilities and outcomes), or two variants of uncertainty – ambiguity (some information not known/knowable) or ignorance (nothing is known about the likelihoods.) Many realistic problems in decision making may fall under ambiguity and ignorance (i.e., unknown probability case) rather than risk (i.e., known probability case).

An important point is that the variant of uncertainty in a task is not an objective property of the task – rather it is the subject's perception of the task and thus reflects his or her current "state of knowledge" about the decision domain. For example, if a decision maker believes that a specific decision task is ambiguous rather than risky, his attitudinal and behavioral responses to the task might vary.

Baron [3] provides a nice discussion of the uncertainty/ambiguity in Chapter 11 of his book. He likens people's responses to ambiguous risks to a "framing" effect - analogous to the loss-gain "framing effects" discussed by Kahneman and Tversky [24]. We prefer this interpretation and thus view the "state of knowledge of a decision maker" as a frame that an online consumer adopts.

The theoretical basis for prior research on risks in behavioral and economic approaches falls into three categories: studies based on utility/decision theory, studies based on attitudinal theories, and studies using the psychometric paradigm. Next, we briefly review the prior IS research on risk and uncertainty with an emphasis on theories.

2.2. Risk studies based on utility theory

Decision theory assumes that the states of the world (e.g., {Rain}, {No Rain}) and acts/decisions (e.g., {Carry an umbrella}, {Carry nothing}) are known to a decision maker. A rational decision maker is assumed to have *consistent preferences,* or equivalently, follow a set of reasonable axioms of choice, such as the seven axioms in the subjective expected utility model (SEU) by Savage [38]. It is then deduced that a consistent preference ordering among acts is identical to the decision maker maximizing a utility function, defined on acts, given a probability distribution over states of the world. Thus, the primitive is the preference ordering among acts and a consistent ordering always implies the existence of a well-defined probability-like measure across the states of the world. That is, a rational person cannot say that he or she has no probability estimate on whether or not it would rain. That is, in terms of the SEU theory, one cannot say "I don't know".

In his classic work, Ellsberg [11] discusses several experiments using urn tasks and shows that even the most sophisticated decision makers (including Savage [38], the founder of the SEU theory) demonstrate inconsistent preferences. Ellsberg proposed *ambiguity* as a third dimension of the choice problem (apart from probability and value) and defined it as “a quality depending on the amount, type, reliability and ‘unanimity’ of information, giving rise to one’s degree of ‘confidence’ in an estimate of relative likelihoods” (p. 657). Research by Ellsberg and several others since then suggests that SEU, the workhorse model used in almost all areas of decision theory, cannot incorporate some notions of not knowing [11, 19, 20].

A general finding on ambiguity is that people are averse to ambiguous situations, that is, people prefer known and specific probabilities to ambiguous or vague estimates. Major explanations for the existence of ambiguity aversion include: i) subjects assuming the worst when probability is unknown [11], ii) a desire to avoid post-purchase regret [33], iii) a feeling that justifying an ambiguous outcome is harder [8], iv) suspicious of the process by which randomness is generated [48], and v) suspicious that subjects are facing a biased task [16]. Ambiguity aversion is strong in contexts where a less ambiguous event is judged together with a more ambiguous event, but is weaker when events are judged in an isolated manner – this is called the comparative ignorance hypothesis by Fox and Tversky [15]. Chow and Sarin [6] show that ambiguity aversion is evident when a decision maker thinks he/she knows less than another. When people feel they are confident about their knowledge of an event, they are less ambiguity averse – this is termed the competence hypothesis by Heath and Tversky [21]. Overall, various context, task and individual factors affect the decision making under ambiguity.

Aquisti and Grossklags [1] is the only IS paper we are aware of that studied the link between online consumers’ privacy decisions and ambiguity, uncertainty, and limited information for privacy decision making. Their experimental study concluded that ambiguity and uncertainty in framing marketing offers increases subjects’ difficulty in predicting consequences of personal information disclosure and decreases their willingness to accept the offers.

The research that is most relevant to our study is by Chow and Sarin [7]. Chow and Sarin focused on a property of knowledge which may be called knowability. They categorized a decision maker's state of knowledge about a task as falling under three levels: known uncertainty (or risk), unknown uncertainty (or ambiguity), or unknowable uncertainty (similar to ignorance). Using an urn task, they induced the three states of knowability about uncertainty in their subjects. Their experimental results show that while people are more averse to unknown and unknowable uncertainties compared to known risks (i.e., ambiguity aversion), they are less averse to unknowable uncertainty than to unknown uncertainty.

2.3. Risk studies based on attitudinal theories

A large amount of prior research on online risks was based on attitudinal theories drawn from social psychology which posit a causal chain such as beliefs->attitudes->intentions->behavior. In TRA (theory of reasoned action) [14], for instance, behavioral intentions, determined by attitudes and perceptions, are antecedents to specific behaviors. For example, an online customer’s perception and attitudes regarding risks may be modeled as beliefs, and will affect his or her behavioral intentions to conduct transactions online. Several IS studies used attitudinal theories to study how risk perception affects a dependent variable such as trust, purchase intention, and etc. These studies include Bhatnagar et al. [4], Miyazaki and Fernandez [29], Salisbury et al. [37], Pavlou [31], Milne et al. [28], Dinev and Hu [10], Jiang et al. [23], and Tsai et al. [46]. Knowledge in these studies generally refers to experience, maturity of subject, user awareness in a general sense, and familiarity with a task. None of the studies, however, explicitly conceptualize decision maker's state of knowledge of risks nor discuss variants of uncertainty.

2.4. The psychometric approach to risks

The psychometric paradigm has been used extensively in studying risk perceptions in various domains. Prior IS research based on the psychometric theory suggests that consumers use many attributes other than risk probabilities and consequences in their decision making.

Fischhoff et al. [13] studied technological risks using the psychometric paradigm with some inclusion of knowledge of risks. Slovic et al. [43] found that risk acceptability is affected by risk attributes, such as familiarity, control, and uncertainty about the risk level. They equated the concept of knowledge of risk to one’s familiarity with the risk level. However, they did not distinguish among the different variants of uncertainty.

Slovic [42] further elaborated the psychometric approach to the study of risk perceptions. He suggested that the level of knowledge attribute seems to influence the relationship between perceived risk, perceived benefit, and risk acceptance. However, he did not elaborate on the knowledge of risk dimension and did not distinguish among different variants of uncertainty. Slovic et al. [42] and Fischoff et al. [13]

are both dated studies and do not discuss security risks spawned by e-commerce.

Nyshadham and Ugbaja [30] and Gabriel and Nyshadham [17] were two IS papers which explicitly used the psychometric paradigm to study online risk perceptions. Using data reduction methods on survey data (Multidimensional Scaling and Factor Analysis, respectively), they found that knowledge of risks is an important dimension in online risk perceptions of subjects. However, they do not provide a conceptualization of knowledge of risks nor discuss variants of uncertainty.

2.5. Summary of literature

An interesting characteristic of most online risks is that their incidence and consequence are poorly understood, even by experts. Our review of existing work suggests that a) some forms of uncertainty cannot be conceptualized under utility theory, b) IS work based on social psychology theories do not address variants of risk or knowledge states of people and c) work under the psychometric paradigm in IS identifies knowledge as a dimension of risk perception but does not discuss variants of risk or knowledge states. In this research, we explicitly recognize variants of uncertainty and speculate on its effects on decisions. The purpose of this research is to study the impact of subjective knowledge of variants of uncertainty on decision making. In the context of B2C ecommerce, a simple model is proposed and tested using an experiment.

3. Research model and hypotheses

We conceptualize knowability, an attribute of uncertainty, as a state of mind of a decision maker. That is, faced with a decision situation involving uncertainty, a decision maker can usually sense which kind of uncertainty is involved. In the context of online risks, we propose that the degree of knowledge a decision maker has regarding an event or task falls under one of four notions of knowability of a risk: known certainty, known uncertainty, unknowable uncertainty, and unknown uncertainty. Table 1 below defines the four degrees of knowledge with examples.

Table 1. Taxonomy of risk knowledge (adapted from Chow and Sarin [7])

Degree of Knowledge	Definition	Example
Known Certainty	Information on all attributes and alternatives are available.	A software vendor guarantees in writing that none of its online transactions leads to identity theft, due to strong online security mechanism.
Known Uncertainty	Risk probability is precisely specified and generally agreed upon.	It is officially confirmed that 3% of online transactions with the software vendor lead to identity theft.
Unknowable Uncertainty	Risk probability is unavailable to all.	No one knows and there is no way to find out exactly what percentage of online transactions with the software vendor lead to identity theft.
Unknown Uncertainty	Risk probability is missing to one but may be possessed by others.	The public is only told that less than 5% online transactions with the software vendor lead to identity theft. But the exact percentage is not disclosed.

Known certainty is probably the knowability state which is most comfortable for decision makers, simply because there is nothing which is unknown or unknowable. Known uncertainty, which Chow and Sarin [7] characterize as known specificity of probability, is identical to risk, and most people would be averse to the introduction of a risk. People need to be paid a certain amount of money to make them indifferent between a certain outcome and a known uncertain outcome (called risk premium in utility theory). The first hypothesis can thus be stated as follows:

Hypothesis 1: Known certainty is preferable to known uncertainty in consumer evaluation of online security risks.

Unknown uncertainty means that the subject believes that some useful information about probability is vague, ambiguous or missing. Thus, a subject who believes that a task involves unknown uncertainty may not feel certain of some critical information at a personal level; however, she may feel that someone else would know enough to resolve the unknown uncertainty into a known uncertainty.

For example, an author of this paper may not know the likelihood of identity theft; however, he firmly believes that such information is available and can be obtained (e.g., triangulating data from several well known databases).

As indicated in the literature review, a consistent empirical finding is that most people are ambiguity averse, with the strength of aversion depending on many context, task and individual factors. Put differently, a gamble under known uncertainty requires a risk premium to make it comparable to a certain outcome, whereas a gamble under unknown uncertainty may require an additional ambiguity premium. The second hypothesis can be stated as follows:

Hypothesis 2: Known uncertainty is preferable to unknown uncertainty in consumer evaluation of online security risks.

Unknowable uncertainty is a rather interesting knowledge state. In this state, a decision maker knows that there is some uncertainty in the decision task and that this uncertainty may never be resolved satisfactorily. That is, if an author of this paper believed that identity theft was of the unknowable uncertainty type, then he would say something to the effect of "I don't know how likely identity theft is, but I am certain there is no way of knowing its likelihood. One might as well live with it."

Chow and Sarin [7] found that people in fact are less averse to unknowable uncertainty than to unknown uncertainty when using objective urn tasks in which information about differently colored balls was manipulated. However, we do not know of any study which used a realistic task in which unknowable uncertainty is studied. Our intuition, supported by Chow and Sarin [7] is that people would judge an unknowable uncertainty ("no one can ever know") as less stressful than unknown uncertainty ("I don't know, but someone might know"). Thus, we state the third hypothesis as follows:

Hypothesis 3: Unknowable uncertainty is preferable to unknown uncertainty in consumer evaluation of online security risks.

The research model is summarized in the diagram in Figure 1 below. In the context of online risks faced by consumers, four types of uncertainty are identified. We assume that, in evaluating a task, a consumer attends to the type of uncertainty first and in that sense, frames the decision task. Evaluation of risk depends on the type of uncertainty as well as the characteristics of the task. In summary, this research proposes that people would prefer Known Certainty to Known Uncertainty to Unknowable Uncertainty to Unknown Uncertainty i.e., KC>KU>UBU>UNU.

Consumers' behavioral response to risks is measured using two well-known measures: a) a willingness to pay (WTP) to avoid the risk and b) an attitudinal measure of intention to purchase (ITP) online given the risk. Prior research shows that decision makers will pay a premium to avoid risk (risk premium) or uncertainty (ambiguity premium) [5, 7, 35]. Willingness to pay is used as a proxy measure for the behavioral variable of the risk premium. The purchase intention construct is extensively used in contexts where a purchase is involved and is proximal to actual behavior (whether or not a good is purchased). In addition, according to the theory of reasoned action (TRA), behavioral intentions, such as purchase intentions, are antecedents to actual individual behaviors and are determined by attitudes and perceptions, including online risk perceptions [10, 14, 31, 37]. In other words, WTP is expected to increase as the perceived risk level grows, whereas ITP is expected to decrease as the perceived risk level increases. Based on the prior research finding on ambiguity aversion [7, 11, 21, 22, 33], we expect WTP to avoid a risk and intention to purchase (ITP) to be negatively correlated. The compound hypothesis can be succinctly stated using ITP as the measure as: ITP(KC)>ITP(KU)>ITP(UBU)>ITP(UNU), with the opposite sign for WTP.

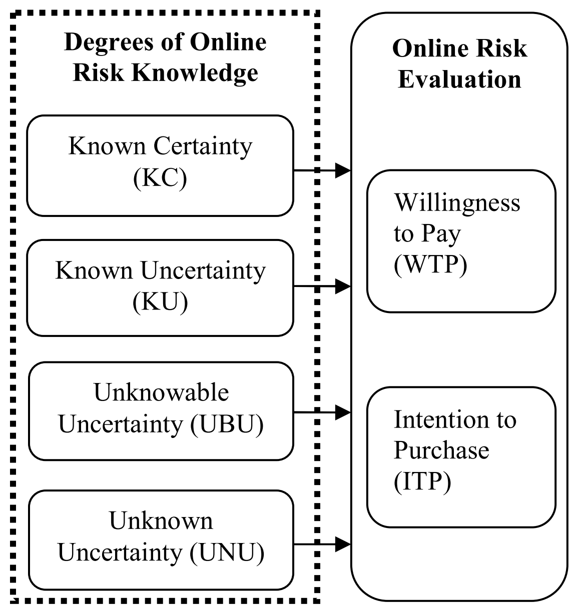

Figure 1. Research model

4. Methodology

4.1. Experimental design

An experiment is used to test the research model.

Knowability or degree of knowledge is the key treatment variable, and WTP and ITP are the primary dependent variables. Aspects of ambiguity, such as degree of confidence, are used as covariates.

4.2. Pilot study

A pilot study was conducted to test and refine the experimental design and to obtain an estimate of the effect size so as to determine the sample size for the main experiment. The pilot used 40 undergraduate student subjects who were recruited from a small college in the Pittsburgh area in northeastern United States. The subjects performed the task online via a secure web site. The four levels of the knowability treatment variable, viz., known certainty (KC), known uncertainty (KU), unknowable uncertainty (UBU), and unknown uncertainty (UNU) were varied across four subgroups of 10 subjects each. A within-subject design was used, with each subject receiving all four treatments, albeit in a different order. While counterbalancing was not used, each treatment level was the first for a subgroup of students.

Prior work in the study of ambiguity typically used objective urn tasks to induce different levels of knowability among subjects [7, 11, 33, 35]. The pilot test was necessary since we are using vignettes containing textual descriptions of risk and these have never been done before. Rather than introduce arbitrary vignettes, we tried to match them to "objective risks as in urn tasks" since these have been studied in literature. This matching also yields a manipulation check. This research is contextualized to online risks and thus, vignettes were developed for each level of the treatment variable. Each subject was asked to read a vignette which described a risk and then provide his numerical estimates of WTP (ratio scale) and ITP (interval scale) based on the transaction value and risk scenario given. The urn tasks from prior research were used as manipulation checks, and subjects were asked to identify the right urn task choice with the given vignette description. Table 2 below shows the treatment variables, vignettes, and manipulation checks.

Data collected from the pilot was analyzed. First, the pilot suggested that the manipulation check (i.e., knowability level induced by an objective urn task and that induced by the context-specific vignettes) did match fairly well. Second, data analysis suggested severe order effects (i.e., the sequence of treatments made a difference). Discussions with subjects also suggested that subjects were confused in moving from one treatment level to another. Thus, it was decided that the main experiment use a between-subjects design wherein each subject is exposed to only a single level of the treatment variable. Third, data from the first vignette each group received and responded to was used to compute an effect size under standard assumptions (alpha = 0.05 and power = 0.8). Calculations using the G*Power analysis software [12] based on the computed effect size suggested a sample size estimate of 40 subjects for each treatment variable for the main experiment. Further, some minor changes were made to the phrasing and formatting of items in the vignette and the questionnaire instrument.

Table 2. Treatment variables, vignettes, and manipulation checks

Treatment Variables: Legend: Knowability levels KU = Known Uncertainty UBU = Unknowable Uncertainty UNU = Unknown Uncertainty KC = Known Certainty	**Manipulation Check: Question:** If the identity theft risk is compared to the chance of randomly drawing a red ball from an urn of 100 red and black balls mixed together, the scenario given resembles which of the following?
KU Treatment Vignette: *A published study concludes that about 3% of online transactions from sites such as E-WizWire eventually lead to identity theft.*	Choices are: a, b, c, d. **Expected Answer:** ***a**. Out of 100 balls in the urn, 3 are red and the rest are black.*
UBU Treatment Vignette: *Research studies have concluded that, while the probability of identity theft occurring due to online transactions with firms like E-WizWire is small, it is not possible to compute a reliable estimate of the rate. Thus, there seems to be no way of knowing the probability of identity theft arising from a transaction.*	Choices are: a, b, c, d. **Expected Answer:** ***b**. Out of 100 balls in the urn, there is no way of knowing how many are red and how many are black.*
UNU Treatment Vignette: *A published summary of a study says that the estimated rate of transaction from firms like E-WizWire leading to identity theft is less than 5%. The study was conducted by a coalition of online vendors, vendors of anti-virus software and computer security firms. The study was privately financed and thus the details of*	Choices are: a, b, c, d. **Expected Answer:** ***c.** Out of 100 balls in the urn, we only know that the number of red balls is below 5. But most people do not know exactly how many are red and how many are black.*

the study are not made available to the public. The exact rate information may be known only to some insiders but unknown to the public.	
KC Treatment Vignette: *E-WizWire guarantees in writing and with full guarantee that none of their online transactions will lead to identity theft, due to their strong online security mechanism. Should it happen that a transaction with E-WizWire leads to an identity theft, the firm will pay all costs involved in resolving the issue at no expense to the user.*	Choices are: a, b, c, d. **Expected Answer:** ***d.*** *It is officially announced that there are no red balls out of the 100 balls in the urn.*

4.3. Main study

A total of 160 student subjects were recruited from a small college in the Pittsburgh area in northeastern United States. The subjects were divided into four groups of 40 each and were randomly assigned to a specific treatment level (knowability). Each group received the vignette which corresponded to a single knowability level from KC (known certainty), KU (known uncertainty), UBU (unknowable uncertainty), and UNU (unknown uncertainty). The subjects participated in the experiment online via a secure web site.

5. Analysis of main study data

The manipulation check question was used to judge if subjects understood the fine-grained distinctions among knowability levels. The responses of a total of seven subjects were deleted based on the manipulation check.

5.1. Descriptive data

Demographic data collected from the subjects included age, gender, Internet usage, and experience in online purchase and online credit card payment. The data shows that subjects were experienced users of the Internet - over 90% of the subjects have had prior experience purchasing online and making payments online by credit card; over 95% of the subjects use the Internet between 1 and 10 hours per day; and over 80% of the subjects have used the Internet for four or more years. The age of the subjects falls between 18 and 50, including 57.5% in age 18-21, 30% in age 22-30, 10% in age 31-40, and 2.5% in age 41-50. 56% of the subjects were female while 44% were male. Table 3 below presents the mean and standard deviation of the primary dependent variables (WTP and ITP) across the four treatments.

Table 3. Descriptive statistics of dependent variables (WTP & ITP)

Treatment	DV	Mean	Standard Deviation
KC (N=40)	WTP	3.5245	2.64311
	ITP	8.2750	1.83956
KU (N=38)	WTP	4.7355	2.56112
	ITP	7.3947	1.91070
UBU (N=38)	WTP	7.1139	4.36347
	ITP	5.3421	2.43040
UNU (N=37)	WTP	8.4932	4.22315
	ITP	4.2703	1.92424

The two dependent measures WTP and ITP, are expected to be correlated negatively - that is, if people are willing to pay more to avoid a risk, then they would also be less intent on purchasing. The correlation data does indicate significant negative correlations between the two measures. The Pearson correlations between WTP and ITP were: -.682 in the KC case (p=.01, N=40), -.334 (p=.01, N=38) for the KU case, -.671 (p=.01, N=38) for the UBU case, and -.435 (p=.01, N=37) for the UNU case.

5.2. Test of hypotheses

The main hypothesis of this study is that subjects prefer known certainty (KC) over known uncertainty (KU) over unknowable uncertainty (UBU) over unknown uncertainty (UNU) in online risk evaluation. In other words, WTP (willingness to pay to avoid risk) increases as the perceived risk level grows, whereas ITP (intention to purchase) decreases.

An ANOVA was conducted with WTP as the dependent variable and knowability level as the treatment variable. The null hypothesis of no difference in WTP across treatments is rejected (F (3, 149), p=.000) with a post-hoc power of close to 1.0. Thus, we conclude that knowability level affects WTP.

Given that knowability level does affect WTP, a Tukey's HSD (Honest Significant Differences) post hoc test was used to determine how the group means differ. The Tukey HSD test is an ANOVA test used to control for Type I error across the multiple pairwise comparisons. Table 4 below summarizes the Tukey HSD test result for WTP across the treatment groups. ANOVA on ITP yielded identical conclusions but is not reported due to space limitations.

Table 4. Tukey HSD Post Hoc Test for WTP

	(I) Treatment	(J) Treatment	Mean Difference (I-J)
Tukey HSD	KC	KU	-1.2110
		UBU	-3.5894*
		UNU	-4.9687*
	KU	KC	1.2110
		UBU	-2.3784*
		UNU	-3.7577*
	UBU	KC	3.5894*
		KU	2.3784*
		UNU	-1.3793
	UNU	KC	4.9687*
		KU	3.7577*
		UBU	1.3793

* The mean difference is significant at the .05 level.

5.3. Analysis and interpretation

When choosing between a KC (known certainty) and a KU (known uncertainty), we expected people to pay a premium to avoid taking on additional risk. Subjects are willing to pay an average of $1.2 to avoid transitioning from KC to KU as shown in Table 4. However, this difference is not statistically significant (p=0.43).

Table 4 also suggests that people are willing to pay a statistically significant amount to avoid moving from cases involving "pure risk" (i.e., KC, KU) to those involving uncertainty/ambiguity (UNU, UBU). Specifically, these amounts are: $3.5 for avoiding transition from KC to UBU, $4.9 for avoiding transition from KC to UNU, $2.4 for avoiding transition from KU to UBU, and $3.8 for avoiding transition from KU to UNU. Thus, there is a clear uncertainty/ambiguity aversion. That is, when probabilities are not specified (as in the UNU-unknown case or UBU-unknowable case), people do recognize that the nature of uncertainty is of a different type and they are willing to pay more to avoid it.

We expected that people would be willing to pay less for an unknowable risk (UBU) than an unknown risk (UNU). Comparing the mean difference from Table 4 for the UNU-unknown and UBU-unknowable cases, we see that subjects on average would pay up to $1.4 to avoid UNU state from UBU state. However, this difference is not statistically significant (p=.33). The experiment's results can be summarized as: KC~KU>UNU~UBU, where ~ indicates no statistically significant difference.

6. Conclusions

Since most risks, especially those related to technology, are difficult to quantify, a question arises as to how decision makers judge and respond to such risks. In this study, we propose that uncertainty is of many types and one dimension across which they can be distinguished is knowability. People can make distinctions between known versus unknown (or known vaguely/imprecisely) versus unknowable information in a given task and use it in their decision process. In the context of B2C e-commerce, we conducted an experiment to study the effect of different levels of consumers' knowledge of a typical online security risk on their purchase behavior. Results suggest that people can distinguish between risk and uncertainty and will pay a premium to avoid uncertainty.

Specifically, the results support *Hypothesis 2* and suggest that the subjects respond to the risk as proposed by the study – they are willing to pay more to avoid the risk and have lower intention to purchase under the unknowable (UBU) and unknown (UNU) risk conditions. However, *Hypothesis 1* (KC>KU) and *Hypothesis 3* (UBU>UNU) in risk preferences are not supported. Chow and Sarin [6] found significant difference in uncertainty preferences between the UBU and UNU conditions – unknowable uncertainty is more preferable than unknown uncertainty. This study did not find such difference between UBU and UNU to be significant. It could be because people do not judge UBU and UNU differently in realistic tasks as opposed to the abstract urn tasks used by Chow and Sarin. It could also be that ambiguity is a norm rather than a special case for decision makers. Or it could mean that different experiments and measures are needed for future research. To make results more generalizable, future research could consider sampling population from wider social and geographical areas.

From a practical standpoint, this research shows that ambiguity aversion exists among the Internet users. This research suggests that, in communicating risks (especially information security risks) to online B2C consumers, a firm is better off presenting risks with precise probability and consequence estimates rather than vague or imprecise probabilities. By framing the decision task as one involving risk rather than one of an ambiguity or unknowability, a firm can lower the consumers' willingness to pay (to avoid the risk) and increase consumers' intention to purchase online.

From a theoretical standpoint, this study discusses decision making under variants of uncertainty and thus can be extended to the study of risks of all types, including not only online security and other risks in B2C environments but also risks in inter- and intra-organizational settings. For example, in a re-insurance setting, Kuenreuther et al. [26] argued that an insurance market may fail due to ambiguity. Ambiguity may be a reason why insurance markets are not well developed for ICT (information, communications, and technology) risks. Future research can also focus on the numerous task and context effects under different variants of uncertainty, a few of which are alluded to in the literature review section of this paper.

7. References

[1] A. Acquisti and J. Grossklags, "Uncertainty, Ambiguity, and Privacy," *Proceedings of the 4th Annual Workshop on Economics and Information Security (WEIS 2005)*, 2005, pp. 1-21.

[2] A. Acquisti and J. Grossklags, "What Can Behavioral Economics Teach Us About Privacy?" In A. Acquisti et al. (Ed.), *Digital Privacy: Theory, Technologies and Practices* (pp. 363-378). London, UK: Auerbach Publications, 2007.

[3] J. Baron, *Thinking and Deciding (4th ed.),* New York: Cambridge University Press, 2008.

[4] A. Bhatnagar, S. Misra, and H.R. Rao, "On Risk, Convenience, and Internet Shopping Behavior," *Communications of the ACM*, vol. 43, no. 11, 2000, pp. 98-105.

[5] C. Camerer and M. Weber, "Recent Developments in Modeling Preferences: Uncertainty and Ambiguity," *Journal of Risk and Uncertainty,* no. 5, 1992, pp. 325–370.

[6] C.C. Chow and R.K. Sarin, "Comparative Ignorance and the Ellsberg Paradox," *The Journal of Risk and Uncertainty,* vol. 22, no. 2, 2001, pp. 129-139.

[7] C.C. Chow and R.K. Sarin, "Known, Unknown, and Unknowable Uncertainties," *Theory and Decision,* no.52, 2002, pp. 127-138.

[8] S.P. Curley, J.F. Yates, and R.A. Abrams, "Psychological Sources of Ambiguity Avoidance," *Organizational Behavior and Human Decision Processes*, no. 38, 1986, pp. 230–256.

[9] T. Dinev and P. Hart, "An Extended Privacy Calculus Model for E-Commerce Transactions," *Information Systems Research*, vol. 17, no. 1, 2006, pp. 61-80.

[10] T. Dinev and Q. Hu, "The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies," *Journal of the Association for Information Systems,* vol. 8, July 2007, pp. 386-408.

[11] D. Ellsberg, "Risk, Ambiguity and the Savage Axioms," *Quarterly Journal of Economics,* no. 75, 1961, pp. 643-669.

[12] F. Faul, E. Erdfelder, A.G. Lang, and A. Buchner, "G*Power 3: A Flexible Statistical Power Analysis Program for the Social, Behavioral, And Biomedical Science," *Behavior Research Methods,* no. 39, 2007, pp. 175-191.

[13] B. Fischhoff, P. Slovic, and S. Lichtenstein, "How Safe is Safe Enough? A Psychometric Study of Attitudes Towards Technological Risks and Benefits," *Policy Sciences*, vol. 9, no. 2, 1978, pp. 127-152.

[14] M. Fishbein and I. Ajzen, *Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research,* Reading, MA: Addison-Wesley, 1975.

[15] C.R. Fox and A. Tversky, "Ambiguity Aversion and Comparative Ignorance," *The Quarterly Journal of Economics*, vol. 110, no. 3, 1995, pp. 585-603.

[16] D. Frisch and J. Baron, "Ambiguity and Rationality," *Journal of Behavioral Decision Making*, no. 1, 1988, pp. 149–157.

[17] I.J. Gabriel and E. Nyshadham, "A Cognitive Map of People's Online Risk Perceptions and Attitudes: An Empirical Study," *Proceedings of the 41st Annual Hawaii International Conference on Systems Sciences,* 2008, Big Island, HI, pp. 274-283.

[18] D. Gefen, E. Karahanna, and D.W. Straub, "Trust and TAM in Online Shopping: An Integrated Model," *MIS Quaterly,* vol. 27, no. 1, 2003, pp. 51-90.

[19] I. Gilboa and D. Schmeidler, "Maxmin Expected Utility with Non-unique Prior," *Journal of Mathematic Economics,* no. 18, 1989, pp.141-153.

[20] Y. Halevy, "Ellsberg Revisited: An Experimental Study. *Econometrica,* vol. 75, no. 2, 2007, pp. 503-536.

[21] C. Heath and A. Tversky, "Preference and Belief: Ambiguity and Competence in Choice under Uncertainty," *The Journal of Risk and Uncertainty,* no.4, 1991, pp. 5-28.

[22] R.M. Hogarth and H. Kunreuther, "Decision Making Under Ignorance: Arguing With Yourself," *The Journal of Risk and Uncertainty,* no. 10, 1995, pp. 15-36.

[23] J. Jiang, C. Chen, and C. Wang, "Knowledge and Trust in E-consumers' Online Shopping Behavior," *International Symposium on Electronic Commerce and Security,* 2008, pp. 652-656.

[24] D. Kahneman and A. Tversky, "Prospect Theory: Analysis of Decision Under Risk," *Econometrica,* vol. 47, no. 2, 1979, pp. 263-292.

[25] J. Kim, K.P. Arnett, and G.F. Templeton, "Securing Personal Information Assets: Testing Antecedents of Behavioral Intentions," *Proceedings of the Fourteenth Americas Conference on Information Systems,* Toronto, Canada, 2008.

[26] H. Kunreuther, J. Meszaros, R.M. Hogarth, and M. Spranca, "Ambiguity and Underwriter Decision Processes," *Journal of Economic Behavior & Organization*, vol. 26, no. 3, 1995, pp. 337-352.

[27] K.C. Laudon and C.G. Traver, *E-commerce: Business, Technology, Society (4th ed.)*, Upper Saddle River, NJ: Prentice Hall, 2008.

[28] G.R. Milne, A.J. Rohm, and S. Bahl, "Consumers' Protection of Online Privacy and Identity," *The Journal of Consumer Affairs,* vol. 38, no.2, pp. 217-232.

[29] A.D. Miyazaki and A. Fernandez, "Consumer Perceptions of Privacy and Security Risks for Online Shopping," *The Journal of Consumer Affairs*, vol. 35, no. 1, 2001, pp. 27-44.

[30] E.A. Nyshadham and M. Ugbaja, "A Study of Ecommerce Risk Perceptions among B2C Consumers: A Two Country Study," *Proceedings of the 19th Bled eConference*, Bled, Slovenia, 2006.

[31] P.A. Pavlou, "Consumer Acceptance of Electronic commerce: Integrating Trust and Risk with the Technology Acceptance Model," *International Journal of Electronic Commerce,* vol. 7, no. 3, 2003, pp. 69-103.

[32] P.A. Pavlou and M. Fygenson, "Understanding and Predicting Electronic Commerce Adoption: An Extension of the Theory of Planned Behavior," *MIS Quarterly,* vol. 30, no. 1, 2006, pp. 115-143.

[33] B.D. Pulford and A.M. Colman, "Size Doesn't Really Matter: Ambiguity Aversion in Ellsberg Urns with Few Balls," *Experimental Psychology,* no.55, 2008, pp. 31-37.

[34] W. Roberds and S.L. Schreft, "Data Breaches and Identity Theft," *Journal of Monetary Economics,* vol. 56, no. 7, 2009, pp. 918-929.

[35] M. Roca, R.M. Hogarth, and A.J. Maule, "Ambiguity Seeking As A Result of the Status Quo Bias," *The Journal of Risk and Uncertainty,* no. 32, 2006, pp. 175-194.

[36] A.F. Salam, H.R. Rao, and C.C. Pegels, "Consumer-Perceived Risk in E-Commerce Transactions", *Communications of the ACM*, vol. 46, no.12, 2003, pp. 325-331.

[37] W.D. Salisbury, R.A. Pearson, A.W. Pearson, and D.W. Miller, "Perceived Security and World Wide Web Purchase Intention," *Industrial Management & Data Systems,* vol. 101, no.4, pp. 165-176.

[38] L.J. Savage, *The Foundations of Statistics*. New York: Wiley, 1954. (Revised and enlarged edition), New York: Dover, 1972.

[39] G. Shafer, "Savage Revisited," *Statistical Science,* vol. 1, no. 4, 1986, pp. 463-501.

[40] M.B. Schmidt and K.P. Arnett, "Spyware: A Little Knowledge Is A Wonderful Thing," *Communications of the ACM*, vol. 48, no. 8, 2008, pp. 67-70.

[41] J. Sinclaire and R. Wilkes, "Perceptions of the Safety of the Internet: Fear and the Future of the Web," *Proceedings of the Twelfth Americas Conference on Information Systems,* Acapulco, Mexico, 2006.

[42] P. Slovic, "Perception of Risk," *Science*, no. 236, 1987, pp. 280-285.

[43] P. Slovic, B. Fischhoff, and S. Lichtenstein, "Why Study Risk Perception?" *Risk Analysis*, vol. 2, no. 2, 1982, pp. 83-93.

[44] J. Son and S.S. Kim, "Internet Users' Information Privacy-protective Responses: A Taxonomy and A Nomological Model," *MIS Quarterly,* vol. 32, no. 3, 2008, pp. 503-529.

[45] B. Suh and I. Han, "The Impact of Customer Trust and Perception of Security Control on the Acceptance of Electronic Commerce," *International Journal of Electronic Commerce,* Vol. 7, No. 3, 2003, pp. 135–161.

[46] J. Tsai, L. Cranor, S. Egelman, and A. Acqusiti, "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study," *Proceedings of the Twenty Eighth International Conference on Information Systems,* Montreal, Canada, 2007, pp. 1-17.

[47] Y. Wu, S. Ryan, and J. Windsor, "Influence of Social Context and Affect on Individuals' Implementation of Information Security Safeguards," *Proceedings of Thirtieth International Conference on Information Systems,* Phoenix, Arizona, 2009.

[48] X. Yan and S. Dai, "Consumer's Online Shopping Influence Factors and Decision-Making Model," *Proceedings of the Fifteenth Americas Conference on Information Systems,* San Francisco, California, 2009.