Value-based Information Privacy Objectives for Internet Commerce

Gurpreet Dhillon, Tiago Oliveira, Romilla Syed

PII:	S0747-5632(18)30275-9
DOI:	10.1016/j.chb.2018.05.043
Reference:	CHB 5552
To appear in:	*Computers in Human Behavior*
Received Date:	22 May 2017
Accepted Date:	31 May 2018

Please cite this article as: Gurpreet Dhillon, Tiago Oliveira, Romilla Syed, Value-based Information Privacy Objectives for Internet Commerce, *Computers in Human Behavior* (2018), doi: 10.1016/j.chb.2018.05.043

Value-based Information Privacy Objectives for Internet Commerce

Gurpreet Dhillon[*]
Professor
gdhillon@uncg.edu
Phone: (336) 334 4901

Department of Information Systems & Supply Chain Management
Bryan School of Business and Economics
The University of North Carolina at Greensboro
Greensboro, NA 27412

Tiago Oliveira
Assistant Professor
toliveira@novaims.unl.pt
Phone: (+351) 213-828-610

NOVA, Information Management School
Campus de Campolide, 1070-312 Lisboa,
Portugal

Romilla Syed
Assistant Professor
Romilla.syed@umb.edu
Phone: (804) 551-8094

College of Management
University of Massachusetts Boston
100 Morrissey Blvd.
Boston, MA 02125-3393
USA

[*] Corresponding Author

Value-based Information Privacy Objectives for Internet Commerce

ABSTRACT

The purpose of this paper is to define information privacy objectives based on values of individuals. The study is informed by the *value-focused thinking* approach that helps generate objectives for strategic decision makers. We employ a sequential mixed method approach in four phases. Phase 1 uses Value Theory to define individual values for information privacy. Using *value-focused thinking* the values are then converted into objectives. The objectives are classified into *means* and *fundamentals* based on their relative importance. In Phases 2 and 3, drawing on 207 and 458 respondents, respectively; we quantitatively define a more parsimonious set of objectives. In Phase 4, using a new sample of 221 respondents, we apply a confirmatory factorial analysis to test the models hypothesized in previous phases. In the final synthesis, a five-factor model of *means* and *fundamental* objectives is presented. Collectively the *means* and *fundamental* objectives for information privacy present a measurement scale, which is useful for researchers and marketers who wish to research how customer attitudes about how privacy influences Internet behavior. The objectives can also be useful for companies to design privacy for Internet Commerce.

Keywords: Information privacy, privacy measurement scale, individual values, value focused thinking, Internet Commerce, multi-method.

Value-based Information Privacy Objectives for Internet Commerce

1. INTRODUCTION

There is a disconnect between how information privacy is handled by Internet Commerce firms and what individuals care about. Many organizations have simply gone ahead and instituted policies that are counterproductive to maintaining the privacy of individuals. Hence it is important to develop some guidance to strategically ensure information privacy in the context of Internet Commerce. In this paper we develop information privacy objectives and present a model of *fundamental* and *means* objectives. The measurement scale is useful for researchers and marketers alike since it allows to assess consumer attitudes about how privacy influences behavior. The objectives and the scale also help companies to define their information privacy policies better.

The importance of individual information privacy concerns in Internet Commerce gained significant attention around the 1999-2000-time frame when the Electronic Privacy Information Center (EPIC) first brought public attention to Doubleclick's proposed business practices for infringement of privacy in an online environment. In 2000, EPIC filed a complaint with the Federal Trade Commission (FTC) alleging privacy violations[1]. At that time DoubleClick had conceded that it respects the privacy of individuals by not connecting personal information with

[1] http://epic.org/privacy/internet/cookies/doubleclickobjection.pdf

online browsing data. Subsequently, DoubleClick was sold to Epsilon in 2006, and then to Google in 2007. In 2013 Google DoubleClick announced that they would be replacing cookies, a forte of DoubleClick, with a unique personal identifier, which would help track consumer movement on the Internet, and thus help Google target advertising more precisely.

From an Internet Commerce perspective, two interesting and confounding issues emerge. **First**, since 1999, not much has changed in the world of privacy in terms of what Internet Commerce firms should do to protect the privacy of their constituents. Companies such as DoubleClick are engaging in exactly the same practices that they were in 1999. Internet Commerce vendors have not taken any concrete steps to either understand consumer concerns about privacy or to ensure adequate protection. **Second**, consumers may have a limited understanding of what they need to protect and how such protection can be brought about. Many a times, measures taken by consumers are extreme and detrimental to the purpose of Internet Commerce. For example, in the light of recent revelation about surveillance and collection of personal information, Pew research found that 91% of consumers agree that they have lost control of how their information is collected and used by companies. Among a sample of 1002 adults, 86% of internet users have removed or masked their digital footprint, whereas 55% of users have taken steps to avoid being observed by people, organizations or the government. At the same time, many express desire to take additional steps for protecting their information[2]. What consumers really require is a delicate balance between too much exposure and disconnecting entirely (Dwoskin, 2014; Turban, et al., 2018). These examples reveal that there is a lack of importance of a strategic orientation in the context of Internet Privacy.

[2] http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/ by Lee Rainie. Reported on September 21, 2016. Accessed on March 31, 2018

This paper is organized as follows. Following this brief introduction, Section 2 presents the theoretical foundations that inform this research. Section 3 discusses the research methodology employed to elicit a parsimonious set of individual values towards Internet Commerce Privacy. By adopting a mixed method approach, this research balances the idiographic and normative forms of knowledge. In Section 4 we discuss the final model and its utility in protecting Internet Commerce Privacy. Finally, Section 5 concludes the paper by identifying practical and theoretical implications; future research directions are also discussed.

2. THEORETICAL FOUNDATIONS

2.1. The Concept of Individual Values

Management theorists have always considered the concept of personal values to be of significance. This is because personal values provide a reference to desirable behavior. This argument has been made by several researchers, including Gregory and Keeney (1994), who use the concept of values in generating policy alternatives. McDaniels and Trousdale (1999) have explicated values to study tourism, and Torkzadeh and Dhillon (2002) have used values to define objectives for Internet Commerce success. The concept of values in IS research can, however, be traced to the work of Rob Kling, when he studied value conflicts in systems development (see, Kling, 1978, 1980). In recent years Kling's work has been carried forward by Allen (2005) and Hedström et al. (2011). There are, however, several other researchers who have studied personal values in the context of IS research - Friedman et al. (2006) studied value-based designs; May, Dhillon and Caldeira (2013) proposed value-based objectives for ERP systems; and Tan and Hunter (2002) suggest Repertory Grids to elicit values for systems analysis and design.

The majority of value-based research, particularly that following Ralph Keeney's tradition, strives to provide better alternatives for strategic decision-making. Scholars have also suggested that behavior is a result of values and attitudes and that values form a basis for strategic decision-making (Connor & Becker, 1975; Homer & Kahle, 1988). Keeney (1992) notes, "values are principles used for evaluation. We use them to evaluate the action or potential consequences of action and inaction" (p. 6) and "values of decision makers are made explicit with objectives" (p. 33). Irrespective of the widely agreed-upon appreciation for personal values and the role these might play in strategic decision making, cynics may argue that the apparently idealistic values could indeed be construed as psychological self-interest (Baier, 1990). Psychological self-interest purports "psychological egoism", a doctrine stating that individuals are only capable of pursuing things that are in their self-interest (Feinberg, 2007). An opposing view to egoism is that of altruistic value structures, which relates to bequest motives and benevolence.

While Keeney (1992) argues that values form a useful basis for defining objectives for strategic decision making, Hemingway and Maclagan (2004) suggest that values get articulated through managerial discretion. Managerial discretion is defined as the freedom to decide what should be done in any given situation. In the literature, three types of discretion have been identified - *formal, unintended, entrepreneurial* (Hemingway & Maclagan, 2004). The definition of objectives and subsequent articulation are important elements in any strategic decision making process.

With respect to Internet Commerce privacy, therefore, it goes without saying that definition and articulation of objectives would not only help consumers traverse through the complex maze, but also enable companies to offer renewed assurances.

2.2. Information Privacy and Internet Commerce

Information systems researchers have been quite involved in the study of information privacy. The extant research falls into three categories: **1)** researchers who have focused on identifying and defining individual privacy concerns; **2)** researchers who propose mechanisms for evaluating costs and benefits of various privacy related practices, and; **3)** researchers who study the socio-psychological makeup of individuals with respect to privacy protection. Collectively all three strands of privacy research have made a significant contribution to our understanding of information privacy protection, may it be in the traditional computing domains, or in the new and emerging Internet-enabled contexts. However, each of these strands of research is not without limitations. Our review of literature (excluding the review papers by Smith et al. (2011) and Bélanger and Crossler (2011)) found a limited emphasis on research that provides decision aids for companies to design information privacy. Majority of the research also falls short of providing mechanisms for consumers to evaluate organizational privacy issues. The apparent gap in this literature forms the basis of our argument that it is essential to understand individual values, which help in defining objectives. Privacy objectives in turn allow corporates to develop value-based information privacy programs and policies. Privacy policies also help consumers adequately evaluate corporate privacy related programs and policies.

Early information systems studies focusing on **Individual privacy concerns** have been undertaken by Mary Culnan and Jeff Smith (e.g. see, Culnan, 1993; Smith, Milberg, & Burke, 1996). Smith et al. (1996) made a significant contribution to the information privacy literature by studying relationships between organizational practices, individual perceptions of the practices and societal responses. Ever since 1996, the majority of information systems research has explored only one of the three proposed elements in Smith et al., *viz.* individual perceptions of organizational practices. Even the reconceptualization of information privacy concerns by Hong and Thong (Kim, 2008) focuses more on perceptions of individuals and how their information is collected and used by websites. In the intervening years, several other scholars have echoed similar concerns (e.g., Culnan & Williams, 2009; Dinev, Xu, Smith, & Hart, 2013; Pavlou, 2011; Solove, 2006). Therefore, it is fair to conclude that the general emphasis of previous research has been on individual privacy concerns as a key determinant for building consumer confidence. Culnan and Armstrong (2009), for example, highlight the importance of procedural fairness. Moores and Dhillon (2003) make a similar argument with respect to the role of privacy seals in e-commerce. Pavlou (2011) synthesizes these concerns and makes a renewed call for studying Internet Commerce privacy.

A related body of research has also examined the impact of privacy concerns on individual behaviors. For example, Buchanan, Paine, Joinson, and Reips (2007) developed the scales for privacy attitude and privacy behavior, such as general caution and technical protection. In another study, Parsons, Calic, and Barca (2016) examined the difference in privacy behavior as manifested by self-disclosure on Facebook between the employees of an Australian government organization and an academic institution. The authors found that government employees were concerned about the cost of self-disclosure, whereas academic employees were motivated by the benefit of self-disclosure. In another study, Hofstra, Corten, and van Tubergen (2016) examined the privacy behavior of adolescent Facebook users. The authors found that peer influence impacts the adolescents' privacy settings. In addition, popular adolescents are more likely to publicly disclose their information whereas low-trust groups opt for private profiles.

Over the years, consumers have come to realize that organizations are indeed going to collect their personal information, may it be through cookies, or the newly-proposed unique identifiers by Google and Microsoft. However, a problem that has perplexed many scholars is how individuals weigh the **cost and benefit of privacy related practices**. This line of inquiry questions how much information a person is willing to share for leveraging benefits of Internet Commerce. In the literature, this is referred to as the privacy calculus (Chellappa & Shivendu, 2007). Lee et al. (2011) evaluate the cost and benefit from both consumer and organizational standpoints. Using a game theoretic approach, Lee et al. conclude that choices for privacy protection "work as competition mitigation mechanisms in personalization." The authors therefore conclude that privacy protection can indeed function as a proactive measure to take advantage of the personal information that is collected by a firm. However, the authors do acknowledge that privacy protection will help companies enter a marketplace through deterrence. The inherent argument is not too dissimilar to that of process fairness proposed by Culnan and Armstrong (1999). Generally, much of the research in this category defines the precursors of privacy paradox and precarious actions towards resolving such a paradox. In particular, the research in this category has studied the effect of the adoption of privacy practices and the utilization of Internet Commerce (see, Awad & Krishnan, 2006; Mallat, 2007; Tang, Hu, & Smith, 2008; Tsai, et al, 2011; Wattal, et al, 2012).

The desire to balance costs and benefits of information privacy and appreciation of consumer privacy concerns has prompted many researchers to evaluate the **socio-psychological aspects of information privacy**. In particular, researchers have considered factors ranging from individual trust to attitudes and perceived usefulness in adopting Internet Commerce, and also whether privacy considerations have been adequately addressed. For instance, Shankar et al. (2002) have argued that understanding online trust can help improve websites and increase consumers' interactions, thus leading to higher profitability. Similarly, Pavlou (2002) explores the role of institution-based trust and how it develops in online B2B marketplaces, so as to increase confidence levels. Dinev and Hart (2006) and Malhotra et al. (2004) have proposed similar arguments, as have Chen and Dhillon (2003), Mai et al. (2010), Tang et al. (2008), Kim (2008), and Li and Unger (2012) in varying contexts. In summary, the socio-psychological line of enquiry has predominantly considered various social and behavioral factors that help in increasing consumer confidence (see, Culnan, 1993).

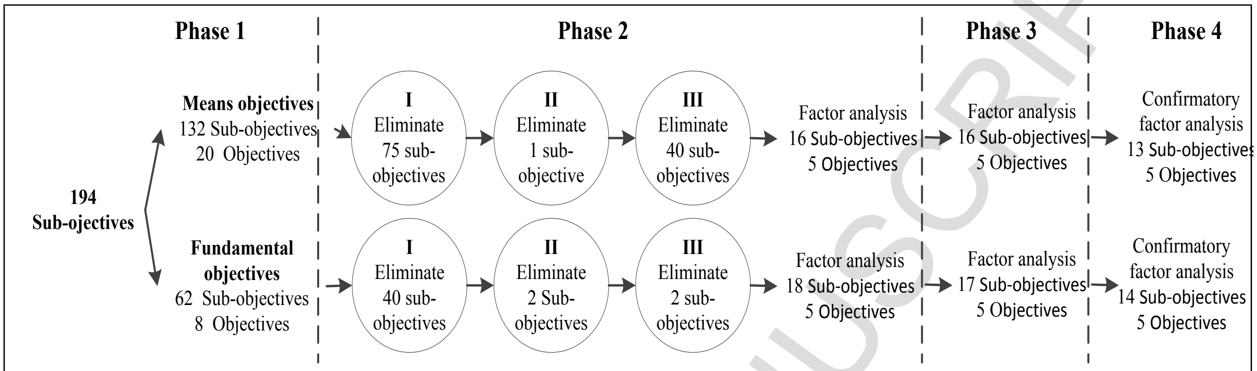
As is evident from our literature review, there has been a limited amount of effort that considers individual values and how these can help organizations to design appropriate information privacy policies and practices. Our literature review also found three major avenues of extending current research in information privacy. **One**: although a plethora of privacy-related research has emanated from a broad range of disciplines, repeated calls are being made to shift the focus of the research community towards the lesser-studied aspects of information privacy. In their literature review, Smith et al. (2011) call for a need for a shift of research focus from normative studies to descriptive or exploratory studies. A similar call is made by Bélanger and Crossler (2011), who argue in favor of "conducting more studies investigating the "why" related to privacy as opposed to the "how." **Two**: imprecise measurement scales have limited the scope of information privacy research. Due to the abundance of inconsistencies and measurement problems, much of the behavioral research uses privacy concerns as a proxy for privacy (Dinev, et al., 2013; Pavlou, 2011). Such concerns have been voiced by many scholars and repeated calls are being made for developing more precise measurement scales (see, Bélanger & Crossler, 2011; Malhotra, et al., 2004; Smith, et al., 1996; Stewart & Segars, 2002). **Three**: much of the existing research conceptualizes privacy as an abstract or an over-arching concept. Solove (2002) advocates the need to recognize the contextual and dynamic nature of privacy within a particular context. Given the strong prospects of extending the research in information privacy, our study is perhaps one of the earliest to heed these calls. The exploratory nature of the research design focuses on individual values about privacy, rather than the concerns. Furthermore, we adopt Solove's view of contextual privacy and attempt to explain it from the perspective of Internet Commerce. And our research presents a measurement scale, which is useful for researchers and marketers who wish to research how customer attitudes about how privacy influences Internet behavior.

3. METHODOLOGY

In this paper we use a sequential mixed method approach by conducting a qualitative study, followed by a series of quantitative phases. The exploratory nature of the qualitative phase allowed us to understand what privacy means in the context of Internet Commerce. It is important to do this, particularly in light of the call made by Pavlou (2011). Internet Commerce privacy objectives derived from the qualitative phase of the study were subsequently confirmed in a three phase quantitative study. The integration of qualitative and quantitative approaches has been espoused in the literature, since it provides a basis for rich meta-inferences (Venkatesh, Brown, & Bala, 2013).

The qualitative phase of the study strictly adhered to Keeney's (1992) value-focused thinking. Several information systems researchers have used value-focused thinking (e.g., see Dhillon & Torkzadeh, 2006; Sheng, Nah, & Siau, 2005), among others. This phase involved eliciting individual values about Internet Commerce privacy and then systematically converting these into means and fundamental objectives. In the quantitative phase of the research, two rounds of factor analysis were undertaken, which was followed by a confirmatory analysis to cross-validate the findings. The sequential methodological design to purify the factors is presented in Figure 1.

Figure 1. Four Phases of Item Purification Process*



Note 1 – Eliminate sub-objectives if item-total correlation were less than 0.5; Note 2 – eliminate sub-objectives if the reliability of the remaining sub-objectives was at least 0.9; III – eliminate sub-objectives that were not pure (loading on more than one factor at 0.30 or above) were also eliminated.

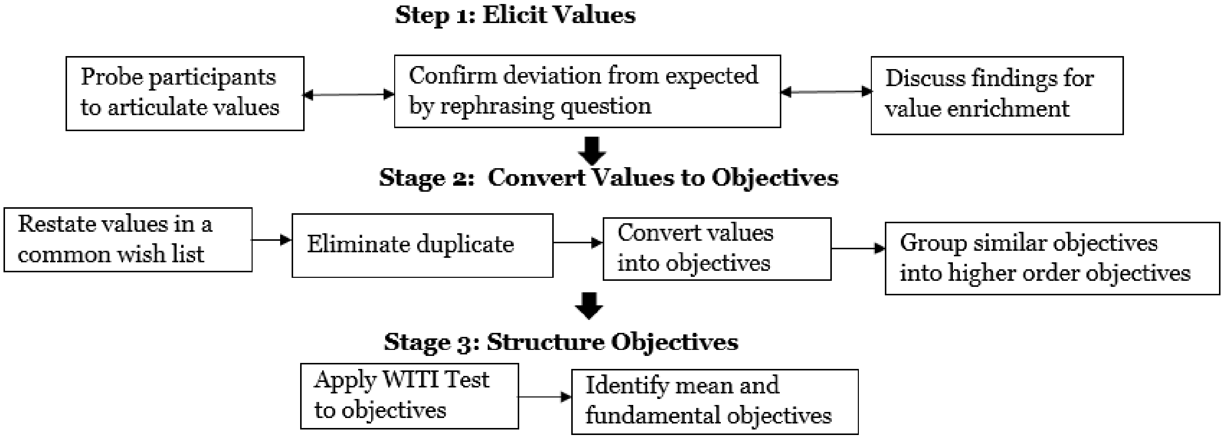
* There was no overlap among the participants of the different phases

3.1. Phase 1

Keeney (1992, 1994) has been a major proponent of value-focused thinking for decision making, as opposed to one based on alternatives. The inherent argument is that alternative-based thinking generates a narrow set of choices, which do not necessarily incorporate values of individuals and the strategic decision makers. The value-focused thinking approach begins with inferring the desires and wishes of individuals in a given decision context[3]. We strictly adhered to the process prescribed by Keeney (1992) and subsequently used by Keeney (1999) and several other scholars (e.g., see Dhillon, et al., 2016; May, et al., 2013). Figure 2 illustrates our qualitative value modeling approach.

[3] A discussion related to comparing alternatives and value-focused thinking is beyond the scope of this paper. A detailed discussion appears in Keeney (1992b) pg. 47-51.

Figure 2. Qualitative value modeling approach


Step 1: Elicit Values
Probe participants to articulate values
Confirm deviation from expected by rephrasing question
Discuss findings for value enrichment
Stage 2: Convert Values to Objectives
Restate values in a common wish list
Eliminate duplicate
Convert values into objectives
Group similar objectives into higher order objectives
Stage 3: Structure Objectives
Apply WITI Test to objectives
Identify mean and fundamental objectives

***Step 1**: Eliciting Values*: In this step, in-depth interviews were conducted. Our criteria for participant selection was twofold: 1) Participant should have experience in using an Internet Commerce website for personal purchases and 2) Participant should have a fair knowledge of consumer privacy. Our respondents were drawn from executives participating in continuing education programs at a large University in the US. All participants had been purchasing products online for at least two years. Fifty-two interviews, each lasting about an hour were conducted. The interviews were recorded and transcribed.

Following Keeney (1992) we used two techniques to conduct the interviews. First, we asked the respondents to create a wish list concerning Internet Commerce privacy. Second, as the interview progressed, we probed the respondents for each of the wishes. Several probing questions were prepared prior to the interview. The probes included questions such as: “If you did not have any constraints, what would you wish for?” "What needs to be changed from the status quo?" "How do you evaluate the level of privacy offered by a given Internet Commerce company?" "What do you expect from the Internet Commerce company?" "How do they tell if the privacy is good or bad?" Apart from asking the interviewees to generate a wish list, they were also asked to create a list of problems and shortcomings in ensuring privacy. In all 337 wishes/problems/concerns were generated.

***Step 2**: Converting Values to Objectives*: In this step, values are converted into a common form. There were several similar sounding values. These are clubbed together to eliminate redundancy. The process allowed us to reduce 337 values into 225 common form values. The comprehensive list of values is then converted into objectives. According to Keeney (1992), an objective is constituted of an object and a directional preference. Keeney describes the structure of an objective as being a verb (direction of change) plus an object (target of change). For example, maximize [verb] privacy [object]. In a final synthesis, a total of 194 objectives were created. In ensuring individual privacy, respondents wanted to achieve these 194 objectives. Nonetheless, some objectives seemed to address a similar issue. Following Keeney, we grouped the related objectives into higher level objectives. This resulted in 28 objectives. Keeney refers to the process of developing and grouping objectives as a means of adequately articulating values and unveiling the meaning. Figure 3 illustrates the process.

Figure 3. Illustration of creating objectives (only partial details are shown)

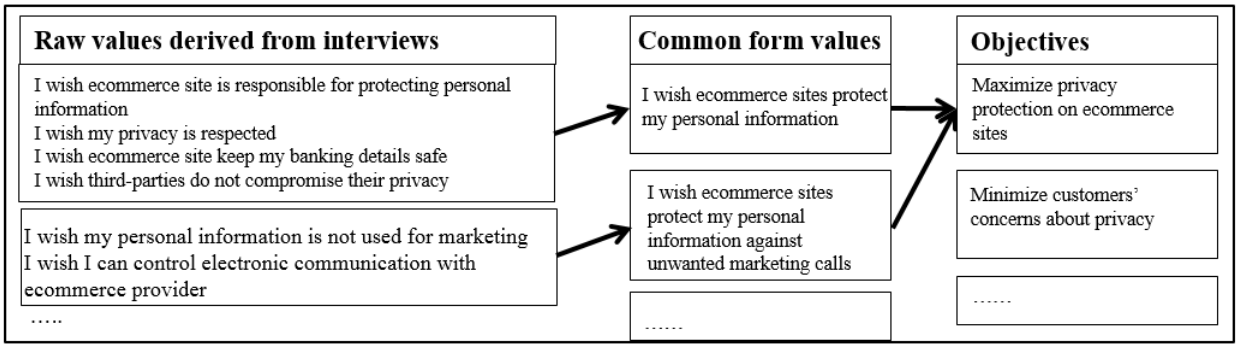

Raw values derived from interviews
I wish ecommerce site is responsible for protecting personal information
I wish my privacy is respected
I wish ecommerce site keep my banking details safe
I wish third-parties do not compromise their privacy
I wish my personal information is not used for marketing
I wish I can control electronic communication with ecommerce provider
…..
Common form values
I wish ecommerce sites protect my personal information
I wish ecommerce sites protect my personal information against unwanted marketing calls
……
Objectives
Maximize privacy protection on ecommerce sites
Minimize customers' concerns about privacy
……

Table 1. Means Objectives (20 objectives, 132 sub-objectives)

Increase Security of Payment Method
Ensure credit card (CC) confidentiality
Maximize transaction security
Standardize online purchasing processes
Minimize accessibility of CC# at point of sale
Maximize security when providing debit card info
Maximize security when providing account details
Ensure transfer of CC details is secure

Maximize Protection of Financial Information
Maximize confidentiality of financial info
Ensure safety of financial info
Minimize CC theft
Ensure security of CC info
Disallow other companies' access to customers' CC details
Ensure account details remain private
Emphasize privacy of financial details
Ensure safety of bank details

Ensure Buyer Anonymity
Maximize shopper anonymity
Maximize web surfer anonymity

Minimize Collection of Information Unrelated to the Transaction
Minimize amount of information collected
Minimize collection of info unrelated to purchase
Minimize information needed for delivery and payment
Provide site access without registration
Ensure shoppers are not asked for SS#
Minimize personal information required
Ensure shoppers' time is not wasted
Minimize retailers' need to know personal details

Increase Respect for the Customers' Data
Emphasize respect for the customers' info
Ensure customers' info is not commoditized
Ensure info deleted when requested by shopper
Emphasize moral and ethical behavior
Increase respect for the consumers' privacy

Stop Shopper Profiling
Provide a profiling free shopping experience
Disallow tracking of purchase activities
Provide a cookie free shopping experience
Minimize use of cookies

Increase System Security Strength
Provide a well-designed system to protect customers' privacy
Maximize security of servers
Ensure quality control of privacy
Maximize security of website
Ensure confidentiality of data
Ensure secure and non-secure data are kept mutually exclusive
Ensure there is no abuse of retailers' protection system
Maximize security after the transaction
Ensure purchase history is secure
Maximize post-transaction security
Maximize use of external audits
Increase use of latest security features
Maximize use of a hierarchy of authorizations
Emphasize the importance of security

Improve Privacy Guarantees
Ensure responsibility for privacy invasions through lawsuits
Provide monetary restitution for privacy breaches
Provide monetary guarantee for mishandling of info
Provide privacy guarantees
Provide financial guarantees for losses
Ensure government involvement
Provide online privacy contract
Provide guarantees of secure transactions
Provide guarantees of post transaction privacy of data
Establish a sovereign body to control privacy
Deemphasize security of CC info because liability is limited

Stop Sharing Customer Info
Ensure personal info never used for purposes other than the transaction
Ensure purchase info is kept private
Strengthen controls over who can access personal info
Ensure that use of purchase information is limited to the individual transaction
Ensure shopper habits are not shared
Minimize exposure of info to other retailers
Emphasize privacy of receipts

Stop the use of Customer "Lists"
Ensure personal info is not put on lists
Disallow use of direct marketing
Disallow solicitations from salespeople
Maximize protection of shoppers' personal info from telemarketers

Minimize Profiting from Customers' Personal Information
Understand personal info is the individual customers' property
Ensure personal info is not sold for profit
Disallow sale of info to database marketing organizations
Disallow sale of personal info to other sites or companies

Minimize Post-Transaction Recordkeeping
Ensure info deleted immediately after transaction
Minimise paper trails
Minimise post-transaction interaction
Decrease need to store CC details

Increase the Strength of Encryption
Ensure secure communications
Ensure secure connections
Maximize use of secure connections on web pages

Enhance Customer I.D. Verification
Maximize use of alternate cutting edge forms of ID verification
Ensure use of encrypted passwords
Ensure adequate purchaser authentication
Improve information collection for order verification
Develop a method besides address validation for payment verification
Emphasize privacy of passwords

Increase Customer Awareness of how Personal Info Handled by Retailer
Increase awareness if retailer is sharing personal info
Promote awareness of how secure personal info is
Increase customers' knowledge of how their personal details are being used

Increase Privacy Policy Awareness
Maximize visibility of privacy policy
Ensure privacy policy is explained at beginning of transaction
Reassure customers that transactions are not being electronically observed
Increase user confidence in the website
Ensure secure certification is used

Understand the Magnitude of Customers' Privacy fears
Minimize importance of privacy
Minimize the expectation of privacy
Downplay privacy fears
Emphasize problem free online shopping experiences
Understand customer concerns about the theft of their info

Decrease Customer Responsibility for Privacy Problems
Increase retailer liability for damage caused by hackers
Increase firms' responsibility for problems created by a lack of privacy
Provide insurance through retailer for any losses resulting from privacy breaches
Ensure compensation for breaches from privacy contract
Minimize hassle to the customer if CC fraud occurs
Minimize the maximum customer loss if CC fraud occurs

Improve the Method of Payment
Provide a better method of payment
Provide the ability to pay by swiping CC on computer
Provide debit accounts at retailer
Minimize inconvenience of canceling CC and getting a new one
Minimize inconvenience of setting up and closing old online purchase acts

Ensure Email Address Confidentiality
Ensure email security

Table 2. Fundamental Objectives (8 objectives, 62 sub-objectives)

Ensure Security of Personal Information
- Ensure confidentiality of personal info
- Ensure privacy of home address
- Ensure security of demographic info
- Ensure security of family info
- Ensure customer info will not be accessible to any other source

Increase Prevention of Fraud
- Ensure criminals have no access to personal info
- Understand the importance of protecting customers' credit
- Ensure customers are not taken advantage of
- Understand identity theft concerns
- Emphasize prevention of identity theft
- Ensure retailer follows through and delivers goods to consumer
- Minimize the possibility of electronic impersonation

Improve the Reputation of the Firm
- Emphasize trust in the retailer
- Emphasize honesty of the retailer
- Emphasize respect for the firm
- Emphasize the firms' reputation
- Enhance company reputation
- Emphasize the integrity of the retailer
- Emphasize trustworthiness of the site
- Improve reputation of brand name
- Ensure retailer fulfills promises

Enhance Shoppers' Ability to Control Personal Data
- Provide option to opt-out of lists
- Provide the option not to be tracked
- Provide the option to not have purchase history put in a database
- Provide control over who views personal info
- Disallow sharing of personal info unless authorized
- Provide the option for discounts if customer allows tracking
- Understand that the customer wants to have a choice in controlling personal info
- Provide customer with the option to delete transaction records
- Ensure purchase info is not shared without first receiving permission

Increase the Discreetness of the Transaction
- Ensure only the customer and retailer know about the transaction
- Ensure a discreet shopping experience
- Maximize use of discreet packaging

Decrease Spam
- Disallow spam
- Provide the option to refuse spam
- Disallow targeted marketing
- Increase the efficiency of marketing efforts
- Understand customers' hatred for spam
- Minimize the advertising that customers' receive
- Disallow sending of spam after purchase
- Minimize potential for spam

Increase the Expectation of Shopping Privately
- Minimize customers' concerns about privacy
- Ensure privacy protection becomes an accepted norm
- Improve privacy policy
- Maximize availability of security info to customers'
- Increase networking with other firms dedicated to privacy
- Provide users with a chance to be part of a safe shopping network of firms

Ensure privacy is consistent with the efficiency of online shopping
- Ensure privacy is consistent with speedy service
- Maximize speed of online purchasing
- Optimize the balance between security and cost
- Enhance functioning of web shopping baskets
- Emphasize low price over privacy
- Maximize efficiency of security measures
- Maximize ease of shopping process

Step 3*: Structuring Objectives*: The resulting 28 objectives were classified into two categories*: means* and *fundamental* objectives. To categorize them, we asked if an objective is an intermediate one, or is more of a fundamental nature. Keeney (1992) recommends the use of the WITI test where the question 'Why is this important?' is repeatedly asked. If the answer to the question suggests another objective, then it is not a candidate for a fundamental objective. Two of the authors independently classified the objectives. The authors then carefully reviewed all objectives and the corresponding clusters, which resulted in 20 means and 8 fundamental objectives. The means and fundamental objectives are present in Tables 1 and 2.

3.2. Phase 2

In Phase 2, based on Boudreau et al. (2001), we conducted an exploratory study to generate a more parsimonious set of means and fundamental objectives for ensuring information privacy in Internet Commerce. A questionnaire based on the 194 sub-objectives (means sub-objectives: 132 questions; fundamental sub-objectives: 62 questions) was designed. Each question is evaluated on a five-point Likert scale, with 1 being "Strongly Disagree" to 5 being "Strongly Agree". The survey was provisioned to graduate and senior undergraduate students at a large public university. A total of 207 usable responses were obtained, with an overall response rate of 85.9%. Among the respondents, 47.8% were male, 52.2% were female, 60.4% were undergraduate, 30.9% were graduate and 8.7% were executive continuing education students. All respondents had online shopping experience and 64.7% of respondents had made more than one online purchase in the last six months.

The analysis of the data had several goals: purification, reliability, unidimensionality, brevity, and simplicity of the factor structure (Torkzadeh & Dhillon, 2002). In this phase we used statistical package for the social sciences (SPSS) software, version 22, for conducted these analyses. Based on Churchill (1979), purification reduces dimensionality. First, we eliminated the sub-objectives if their corrected item-total correlation was less than 0.5. Next, we eliminated a sub-objective if the reliability of the remaining ones was at least 0.9. We calculated Cronbach's α to determine if additional sub-objectives could be eliminated without substantially lowering the reliability. Finally, we conducted factor analyses to assess unidimensionality (Weiss, 1970).

For means objectives, 75 sub-objectives had corrected item-total correlation less than 0.5, which allowed us to reduce the sub-objectives from 132 to 57. The reliability analysis resulted in the elimination of one more sub-objective. Lastly, factor analysis resulted in the elimination of another 40 sub-objectives. Table 3 presents the results of the factors analysis using varimax rotation. Bartlett's test of sphericity is 1670.36 (p < 0.001). KMO measure of the sampling adequacy of the correlation matrix for factor analysis is 0.81, which is strong. For fundamental sub-objectives, corrected item-total correlation criterion (>0.5) led to the elimination of 40 of the 62 sub-objectives. The second criterion, reliability analysis, allowed to eliminate two more sub-objectives. Finally, the factor analysis suggested the elimination of two more sub-objectives. The result of the factor analysis using varimax rotation is presented in Table 4. Bartlett's test of sphericity is 1876.24 (p < 0.001). The value of KMO is 0.85, which is strong.

Table 3. Factor pattern for measures of means objectives (n=207)

	Factor					Corrected Item-Total Correlation
	1	2	3	4	5	
Maximize security of operational systems						
Maximize security after the transaction	**0.87**	0.07	0.14	0.11	0.08	0.79
Maximize transaction security	**0.84**	0.04	0.17	0.12	-0.06	0.79
Maximize security of website	**0.66**	0.07	0.18	0.12	-0.09	0.65
Maximize Protection of Financial Information	**0.63**	0.05	0.13	0.15	-0.05	0.60
Maximize post-transaction security	**0.55**	0.14	0.23	0.15	0.05	0.56
Minimize unwarranted solicitations						
Disallow use of direct marketing	0.08	**0.90**	0.04	0.13	0.22	0.79
Disallow solicitations from salespeople	0.02	**0.79**	0.06	0.22	0.10	0.73
Disallow tracking of purchase activities	0.27	**0.61**	0.15	0.25	0.12	0.64
Improve privacy guarantees						
Provide guarantees of secure transactions	0.26	0.05	**0.78**	-0.02	-0.03	0.69
Provide privacy guarantees	0.24	0.03	**0.73**	0.12	-0.03	0.66
Provide financial guarantees for losses	0.16	0.13	**0.71**	0.17	0.15	0.65
Ensure buyer anonymity						
Maximize shopper anonymity	0.20	0.20	0.10	**0.81**	0.02	0.70
Maximize web surfer anonymity	0.27	0.15	0.04	**0.73**	0.23	0.67
Ensure Buyer Anonymity	0.12	0.24	0.14	**0.54**	0.16	0.56
Understand magnitude of customers' privacy fears						
Minimize importance of privacy	-0.06	0.16	0.03	0.17	**0.90**	0.78
Downplay privacy fears	-0.04	0.20	0.03	0.13	**0.80**	0.78
Eigenvalue	5.22	2.75	1.52	1.24	1.12	-
% Variance						-
Total Variance explained by five factors 74.11%	32.6%	17.2%	9.51%	7.8%	7.0%	

Table 4. Factor pattern for measures of fundamental objectives (n=207)

	Factor					Corrected Item-Total Correlation
	1	2	3	4	5	
Maximize reputation of Internet Commerce vendor						
Emphasize trust in the retailer	**0.88**	0.13	0.14	0.00	0.09	0.82
Emphasize honesty of the retailer	**0.81**	0.06	0.18	-0.02	0.10	0.75
Emphasize the integrity of the retailer	**0.80**	0.14	0.15	0.10	0.09	0.77
Emphasize trustworthiness of the site	**0.69**	0.07	0.15	0.04	0.14	0.66
Emphasize respect for the firm	**0.65**	0.17	0.11	0.26	0.03	0.69
Emphasize the firms' reputation	**0.65**	0.10	0.17	0.21	0.04	0.67
Enhance company reputation	**0.52**	0.20	0.12	0.15	0.02	0.56

Decrease spam						
Disallow spam	0.11	**0.93**	0.10	0.06	0.09	0.79
Decrease Spam	0.09	**0.73**	0.17	0.09	0.04	0.68
Disallow sending of spam after purchase	0.18	**0.62**	0.08	0.08	0.10	0.60
Minimize potential for spam	0.25	**0.54**	0.20	0.20	0.27	0.58
Maximize security of personal information						
Ensure Security of Personal Information	0.20	0.21	**0.88**	0.11	0.12	0.73
Ensure security of family info	0.26	0.21	**0.61**	0.17	0.14	0.54
Ensure confidentiality of personal info	0.29	0.08	**0.52**	0.07	0.18	0.63
Maximize privacy relative to online shopping						
Ensure privacy is consistent with the efficiency of online shopping	0.17	0.12	0.22	**0.78**	0.06	0.66
Ensure privacy is consistent with speedy service	0.14	0.13	0.04	**0.76**	0.00	0.66
Enhance shoppers' ability to control personal data						
Provide the option not to be tracked	0.02	0.17	0.13	0.08	**0.81**	0.51
Provide option to opt-out of lists	0.18	0.09	0.16	-0.03	**0.59**	0.51
Eigenvalue	6.431	2.198	1.504	1.401	1.078	-
% Variance	35.7%	12.2%	8.4%	7.8%	6.0%	-
Total Variance explained by five factors 70.01%						

For both means and fundamental objectives, we used the Kaiser-Guttman rule (also referred to as Kaiser criterion or eigenvalue > 1 rule) (Brown, 2014), i.e., eigenvalue greater than one to retain objectives. For means objectives, according to the criteria, five objectives were retained which explains 74.11% of the total variance. Using a factor-loading threshold of 0.50, the five means objectives are named as: *maximize security of operational systems*; *ensure buyer anonymity*; *minimize unwarranted solicitations*; *understand the magnitude of customers' privacy fears*, and; *improve privacy guarantee*. Likewise, four fundamental objectives were retained, which explain a total of 70.01% variance. Using a factor loading threshold of 0.50, the five objectives are named as: *maximize reputation of Internet Commerce vendor*; *decrease spam*; *maximize security of personal information*; *maximize privacy relative to online shopping*, and; *enhance shoppers' ability to control personal data*.

3.4. Phase 3

Phase 3 was commissioned four months after Phase 2, where we undertook another round of exploratory factor analysis. The purpose of this phase was to validate the factor structure generated in the preceding phase and to increase the generalizability of the instrument. The instructions and questionnaire were the same as in Phase 2. The survey was provisioned to another set of graduate and undergraduate students at the same University. Although, the participation in this survey was voluntary, a total of 458 usable responses were obtained with an overall response rate of 87.9%. Among the respondents, 48.9% were males, 51.1% were females, 41.0% undergraduate, 45.6% graduate, and 13.3% executive. All participants had experience in online engagement and 76.2% had shopped online.

In order to be consistent with Phase 2, we applied two exploratory factor analyses, one for the variables measuring means objectives and the other for the variables measuring fundamental objectives. The exploratory factor analyses were conducted using SPSS software, version 22. The sample size was adequate and larger than the minimum requirement of 10 cases per variable (29:1 for means sub-objectives and 27:1 for fundamental sub-objectives) (Cattell, 2012; Everitt, 1975; Kerlinger, 1978 ; MacCallum, Widaman, Zhang, & Hong, 1999)[4]. We also estimated the internal consistency (corrected item-total correlation) and reliability (alpha) for the two proposed instruments. Lastly, the correlation matrix for each instrument was analyzed for convergent and discriminant validity. The convergent validity was tested if the correlations between measures of the same theoretical objective are different than zero and large enough to warrant further investigation (Campbell & Fiske, 1959). The discriminant validity was tested for each sub-objective by counting the number of times it correlates more highly with a sub-objective of another objective than with sub-objectives of its own theoretical objective, i.e. a variable (Doll & Torkzadeh, 1988).

[4] For detail explanation of sample size effect in factor analysis please see MacCallum, et al. (1999) and Browne (1968).

Just like Phase 2, the criteria for retaining factors for both mean and fundamental objectives is an eigenvalue greater than one (Brown, 2014). For means objectives, using varimax rotation, we obtained five objectives with an eigenvalue greater than one. We tried other rotations, such as quartimax and oblimin, however factor structure for the objectives didn't change. Bartlett's test is statistically significant ($p < 0.001$) and the KMO is 0.80, which is strong. Likewise, for fundamental objectives we applied a factor analysis using varimax rotation; other rotations were applied but the results are analogous to the ones obtained in Phase 2. Bartlett's test is statistically significant ($p < 0.001$) and the KMO is 0.81, which is again strong.

The results corroborate the factor structure of means objectives obtained in Phase 2. The five objectives explained 72% of the variance. Using a factor loading threshold of 0.50, the five objectives are: *maximize security of operational system*; *ensure buyer anonymity*; *minimize unwarranted solicitations*; *understand the magnitude of customers' privacy fears*, and; *improve privacy guarantees*. In Table 5, we present the corrected item-total correlation for each sub-objective of all objectives, all are higher than 0.5. This means that the sub-objectives belong to respective objectives (see, Churchill, 1979). The overall reliability for the 16 items scale is 0.82, which exceeds the suggested cutoff value of 0.70 (Nunnally, 1978). For convergent and discriminant validity, we analyzed the instrument's correlation matrix. Table 6 presents the correlation matrix, means and standard deviation measures of sub-objectives. For the convergent validity test, we analyzed the smallest correlations within each objective; all are statistically significant ($p < 0.001$) and large enough to encourage further investigation (Campbell & Fiske, 1959). With respect to discriminant validity, all 16 sub-objectives are highly correlated with other sub-objectives corresponding to a particular objective (values in bold) than with any sub-objectives of other objectives. This means that there are zero violations (out of 240 comparisons) of discriminant validity conditions.

Table 5. Factor pattern for measures of means objectives (n=458)

	Factor					**Corrected Item-Total Correlation**
	1	**2**	**3**	**4**	**5**	
Maximize security of operational systems						
Maximize security after the transaction (FMO1_1)	**0.83**	0.12	0.07	0.03	0.13	0.77
Maximize transaction security (FMO1_2)	**0.85**	0.08	0.05	-0.09	0.17	0.78
Maximize security of website (FMO1_3	**0.68**	0.10	0.04	-0.15	0.18	0.66
Maximize Protection of Financial Information (FMO1_4)	**0.60**	0.14	0.06	-0.11	0.18	0.59
Maximize post-transaction security (FMO1_5)	**0.59**	0.17	0.11	0.04	0.18	0.58
Ensure buyer anonymity						
Maximize shopper anonymity (FMO2_1)	0.15	**0.86**	0.16	0.03	0.05	0.75
Maximize web surfer anonymity (FMO2_2)	0.19	**0.71**	0.22	0.08	0.06	0.67
Ensure Buyer Anonymity (FMO2_3)	0.13	**0.66**	0.18	0.07	0.12	0.63
Minimize unwarranted solicitations						
Disallow use of direct marketing (FMO3_1)	0.04	0.16	**0.87**	0.14	0.01	0.73
Disallow solicitations from salespeople (FMO3_2)	0.06	0.18	**0.81**	0.10	0.06	0.72
Disallow tracking of purchase activities (FMO3_3)	0.16	0.22	**0.53**	0.06	0.16	0.54
Understand the magnitude of customers' privacy fears						
Minimize importance of privacy (FMO4_1)	-0.10	0.09	0.13	**0.88**	-0.03	0.80
Downplay privacy fears (FMO4_2)	-0.10	0.07	0.13	**0.86**	-0.03	0.80
Improve privacy guarantees						
Provide guarantees of secure transactions (FMO5_1)	0.26	-0.07	0.08	-0.04	**0.73**	0.60
Provide privacy guarantees (FMO5_2)	0.21	0.14	0.00	-0.05	**0.71**	0.58
Provide financial guarantees for losses (FMO5_3)	0.19	0.16	0.15	0.03	**0.58**	0.53
Eigenvalue	4.73	2.78	1.45	1.33	1.25	-
% Variance **Total Variance explained by five factors 72.10%**	29.5%	17.4%	9.1%	8.3%	7.8%	-

Table 6. Correlation matrix of measures of means objectives (n=458)

Items	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**
(1) FMO1_1																
(2) FMO1_2	**0.72**															
(3) FMO1_3	**0.54**	**0.66**														
(4) FMO1_4	**0.54**	**0.59**	**0.51**													
(5) FMO1_5	**0.63**	**0.51**	**0.45**	**0.33**												
(6) FMO2_1	0.26	0.22	0.18	0.22	0.26											
(7) FMO2_2	0.26	0.21	0.25	0.22	0.29	**0.69**										
(8) FMO2_3	0.20	0.21	0.17	0.21	0.22	**0.63**	**0.53**									
(9) FMO3_1	0.12	0.07	0.06	0.06	0.17	0.29	0.32	0.27								
(10) FMO3_2	0.13	0.10	0.08	0.10	0.19	0.30	0.32	0.28	**0.74**							
(11) FMO3_3	0.22	0.21	0.18	0.22	0.17	0.29	0.31	0.30	**0.52**	**0.50**						
(12) FMO4_1	-0.04	-0.15	-0.19	-0.13	-0.01	0.11	0.16	0.11	0.24	0.19	0.14					
(13) FMO4_2	-0.05	-0.14	-0.18	-0.14	-0.01	0.09	0.12	0.13	0.24	0.20	0.11	**0.80**				
(14) FMO5_1	0.32	0.34	0.30	0.27	0.28	0.05	0.05	0.08	0.07	0.12	0.16	-0.08	-0.08			
(15) FMO5_2	0.27	0.30	0.29	0.29	0.30	0.18	0.17	0.21	0.02	0.07	0.20	-0.08	-0.08	**0.56**		
(16) FMO5_3	0.26	0.28	0.26	0.24	0.24	0.21	0.23	0.22	0.18	0.18	0.24	0.01	0.03	**0.48**	**0.46**	
Mean	4.61	4.70	4.62	4.70	4.52	4.10	3.91	4.07	3.41	3.65	3.79	2.56	2.71	4.71	4.62	4.45
Sdev	0.62	0.54	0.56	0.60	0.64	0.95	0.93	1.00	1.13	1.04	1.08	1.59	1.45	0.54	0.61	0.74

Likewise, for fundamental objectives, the five objectives were exactly the same as those derived in Phase 2. Thus, the findings corroborate the instrument obtained in Phase 2. The five objectives explain a total of 70% of the variation. Again, using a factor loading threshold of 0.50, the objectives are named: *maximize reputation of Internet Commerce vendor*; *decrease spam*; *maximize security of personal information*; *maximize privacy relative to online shopping*, and; *enhance shoppers' ability to control personal data.* As shown in Table 7, the corrected item-total correlation is higher than 0.5. The overall reliability for the 17 item scale was 0.84, which exceeds the cutoff value of 0.7 suggested by Nunnally (1978). The correlation matrix of the 17 items (see Table 8) suggests convergent and discriminant validity. To test convergent validity, we analyzed the smallest correlation within objectives; all are statistically significant (p < 0.001) and large enough to encourage further investigation. The examination of the correlation matrix indicate zero violations (out of 272 comparisons) of discriminant validity (see, Campbell & Fiske, 1959), i.e. all 17 sub-objectives are highly correlated with the other sub-objectives corresponding to a particular objective, rather than with any sub-objective of other objectives.

Table 7. Factor pattern for measures of fundamental objectives (n=458)

	Factor					Corrected Item-Total Correlation
	1	2	3	4	5	
Maximize reputation of Internet Commerce vendor						
Emphasize trust in the retailer (FFO1_1)	**0.87**	0.02	0.11	-0.01	0.01	0.79
Emphasize honesty of the retailer (FFO1_2)	**0.83**	0.05	0.11	-0.04	-0.02	0.75
Emphasize the integrity of the retailer (FFO1_3)	**0.82**	0.05	0.10	0.02	0.03	0.76
Emphasize trustworthiness of the site (FFO1_4)	**0.68**	0.05	0.11	0.02	0.00	0.64
Emphasize respect for the firm (FFO1_5)	**0.67**	0.07	0.05	0.24	0.04	0.66
Emphasize the firms' reputation (FFO1_6)	**0.65**	0.00	0.09	0.17	0.03	0.65
Enhance company reputation (FFO1_7)	**0.55**	0.10	0.00	0.07	0.06	0.54
Decrease spam						
Disallow spam (FFO2_1)	0.06	**0.94**	0.10	0.07	0.09	0.77
Disallow sending of spam after purchase (FFO2_2)	0.08	**0.72**	0.11	0.10	0.09	0.68
Decrease Spam (FFO2_3)	0.07	**0.65**	0.12	0.04	0.16	0.62
Maximize security of personal information						
Ensure Security of Personal Information (FFO3_1)	0.10	0.14	**0.92**	0.11	0.06	0.74
Ensure security of family info (FFO3_2)	0.14	0.20	**0.64**	0.21	0.12	0.60
Ensure confidentiality of personal info (FFO3_3)	0.12	0.04	**0.57**	0.09	0.18	0.52
Maximize privacy relative to online shopping						

Ensure privacy is consistent with speedy service (FFO4_1)	0.12	0.09	0.11	**0.85**	-0.01	0.66
Ensure privacy is consistent with the efficiency of online shopping (FFO4_1)	0.13	0.10	0.28	**0.68**	0.07	0.66
Enhance shoppers' ability to control personal data						
Provide option to opt-out of lists (FFO5_1)	0.04	0.12	0.11	0.03	**0.72**	0.55
Provide the option not to be tracked (FFO5_2)	0.02	0.18	0.18	0.02	**0.70**	0.55
Eigenvalue	5.00	2.77	1.66	1.38	1.11	-
% Variance	29.4 %	16.3 %	9.8 %	8.1 %	6.5 %	-
Total Variance explained by five factors 70.01%						

Table 8. Correlation matrix of measures of fundamental objectives (n=458)

Items	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
(1) FFO1_1																	
(2) FFO1_2	**0.81**																
(3) FFO1_3	**0.77**	**0.78**															
(4) FFO1_4	**0.63**	**0.58**	**0.57**														
(5) FFO1_5	**0.48**	**0.44**	**0.51**	**0.46**													
(6) FFO1_6	**0.54**	**0.52**	**0.51**	**0.41**	**0.63**												
(7) FFO1_7	**0.42**	**0.38**	**0.39**	**0.38**	**0.56**	**0.48**											
(8) FFO2_1	0.09	0.11	0.12	0.09	0.06	0.13	0.13										
(9) FFO2_2	0.09	0.13	0.11	0.12	0.08	0.15	0.11	**0.71**									
(10) FFO2_3	0.09	0.07	0.12	0.08	0.06	0.11	0.19	**0.63**	**0.51**								
(11) FFO3_1	0.18	0.18	0.16	0.18	0.20	0.17	0.10	0.24	0.21	0.22							
(12) FFO3_2	0.20	0.19	0.22	0.16	0.19	0.20	0.09	0.29	0.26	0.23	**0.67**						
(13) FFO3_3	0.15	0.14	0.15	0.16	0.17	0.14	0.10	0.10	0.15	0.15	**0.57**	**0.40**					
(14) FFO4_1	0.13	0.11	0.15	0.11	0.21	0.27	0.12	0.18	0.17	0.09	0.23	0.29	0.11				
(15) FFO4_2	0.16	0.14	0.18	0.17	0.18	0.25	0.08	0.18	0.18	0.17	0.32	0.37	0.30	**0.66**			
(16) FFO5_1	0.07	0.04	0.09	0.03	0.04	0.09	0.07	0.17	0.19	0.22	0.17	0.20	0.18	0.05	0.11		
(17) FFO5_2	0.05	0.05	0.06	0.06	0.05	0.04	0.07	0.28	0.20	0.23	0.23	0.24	0.25	0.06	0.13	**0.55**	
Mean	3.94	3.95	3.90	4.13	3.79	3.72	3.67	4.10	4.12	4.22	4.66	4.53	4.65	3.90	4.23	4.01	4.02
Sdev	0.95	0.93	0.93	0.86	0.93	0.92	1.03	0.96	0.93	0.88	0.59	0.69	0.64	1.05	0.89	1.00	1.04

3.4. Phase 4

In Phase 4, which was initiated after another six months, we undertook a confirmatory factor analysis to check the coherence of *a priori* factor structure for both means and fundamental objectives derived in preceding phase. The survey was administered to graduate and undergraduate students at the same University. The participation was completely voluntary. A total of 221 usable responses (89 male and 132 female) were obtained with an overall response rate of 92.5%. The respondents included 40% males, 60% were females, 54.7% undergraduate, 35.3% graduate, and 10.0% executive level students. All participants had experience in online research and 74.6% had shopped online in the last six months. This reveals that the respondents were qualified to participate in the survey.

We applied two-factor analysis corresponding to the two instruments for means and fundamental objectives developed in the last phase. The purpose of this analysis is to re-examine the specification and estimations of the proposed models (see, Bollen, 1989). If the factor structures replicate, then it is prudent to continue with a confirmatory factorial analysis (CFA). The CFA were conducted using analysis of moment structures (AMOS) software, version 21. To measure developments, an iterative process is necessary, i.e., examining measurement properties to purify and re-specify scales and developing rigorous measures (Chang, Torkzadeh, & Dhillon, 2004; Churchill, 1979; Segars, 1997). Segars and Grover (1998), with respect to measurement properties, suggest, "measured factors be modeled in isolation, then in pairs, and then as a collective network" (p. 148). This allows for measurement efficiency and avoid problems caused by excessive error in the measurement (Anderson, 1987; Anderson & Gerbing, 1988; Segars & Grover, 1993).

For each objective, we tested the convergent validity and unidimensionality. First, for each objective with more than the sub-objectives, we eliminated sub-objectives with low loadings. Then we examined the modification indices to identify possible error correlation that might improve model fit. This was followed by testing pair objectives to identify cross-loadings, and thus to ensure the unidimensionality of each objective. Cross-loading of sub-objective with respect to all objectives was also examined, i.e. a full measurement model. We also computed average variance extracted (AVE). Values higher than the threshold of 0.50 indicate that the measurement error is smaller than the variance captured by the construct (Hair, 2010). This procedure established both convergent validity and unidimensionality of each objective. Secondly, construct reliability was tested by computing composite factor reliability. Composite reliability assesses whether the sub-objectives are sufficient in representing the respective objective; a common lower threshold of 0.70 is used (Hair, 2010). Finally, discriminant validity was tested based on two criteria. First, we compared the model fit of an unconstrained model (or "frees") that estimates the correlation between a pair of objectives and a constrained model that fixes the correlation between the objectives to unity. Discriminant validity is achieved in case the unconstrained model is significantly better fit than the constrained model. Second, the square root of AVE for each objective should be greater than the correlations with all objectives (Fornell & Larcker, 1981). These results suggest that the sub-objectives share more common variance with their respective objectives than any variance the objective shares with other objectives.

Table 9. Factor pattern for measures of means objectives (n=221)

	Factor loading	**Standard error**	**t-Value**	**R^2**
Maximize security of operational systems				
Maximize security after the transaction (FMO1_1)	0.850	-	-	0.72
Maximize transaction security (FMO1_2)	0.876	0.055	15.7	0.77
Maximize security of website (FMO1_3	0.689	0.069	11.3	0.48
Maximize protection of financial information (FMO1_4)	0.758	0.066	12.9	0.57
Ensure buyer anonymity				
Maximize shopper anonymity (FMO2_1)	0.903	-	-	0.81
Maximize web surfer anonymity (FMO2_2)	0.734	0.068	11.8	0.54
Ensure Buyer Anonymity (FMO2_3)	0.779	0.070	12.6	0.61
Minimize unwarranted solicitations				
Disallow use of direct marketing (FMO3_1)	0.815	-	-	0.67
Disallow solicitations from salespeople (FMO3_2)	0.832	0.116	8.6	0.69
Understand the magnitude of customers' privacy fears				
Minimize importance of privacy (FMO4_1)	0.916	-	-	0.84
Downplay privacy fears (FMO4_2)	0.888	0.106	8.9	0.79
Improve privacy guarantees				
Provide guarantees of secure transactions (FMO5_1)	0.847	-	-	0.72
Provide privacy guarantees (FMO5_2)	0.860	0.098	11.9	0.74
Goodness-of-fit indices:				
χ^2/d.f. = 1.59 (<3); TLI = 0.970 (>0.90); NFI = 0.945 (>0.90); CFI = 0.979 (>0.90); IFI = 0.979 (>0.90); GFI = 0.944 (>0.90); AGFI = 0.907 (>0.90); RMSEA = 0.052 (<0.07);				

For means objectives, exploratory factor analysis confirmed the same structure that was obtained in Phase 3. We eliminated two of the objectives with low loadings: *disallow tracking of purchase activities* and *provide financial guarantees for losses*. Next, we applied a confirmatory factor analysis. For one of the objectives more than three sub-objectives were loaded. However, further analysis of this objective suggested several error correlations. The sub-objective *maximize post-transaction security* contains error correlation with the sub-objectives *maximize protection of financial information* and *maximize transaction security*. Consequently, we eliminated the sub-objective *maximize post-transaction security*. To establish unidimensionality, we analyzed objectives pair-wise. We did not find any cross loading. We then tested the full measured model. As shown in Table 9, the final instrument for means objectives has 5 objectives, with 13 sub-objectives. The goodness-of-fit was checked with the respective cutoff for a satisfactory fit, i.e., the: χ^2/d.f. should be lower than 3 (Kline, 2005); Tucker-Lewis Index (TLI) greater than 0.90 (Awang, 2012; Forza & Filippini, 1998); normed fit index (NFI) greater than 0.90 (Awang 2012); confirmatory fit index (CFI) of greater than 0.90 (Awang, 2012; Joseph F Hair, Black, Babin, Anderson, & Tatham, 2010). Incremental fit index (IFI) should be larger than 0.9 (Baumgartner & Homburg, 1996); Goodness-of-fit index (GFI) greater than 0.90 (Awang, 2012; Hair, et al., 2010); adjusted goodness-of-fit index (AGFI) should be larger than 0.9 (Baumgartner & Homburg, 1996); root mean square error of approximation (RMSEA) should be less than 0.07 (Steiger, 2007). Based on Table 9, the goodness-of-fit indices for all measure are better than respective cutoffs. AVE was higher than 0.5 for all objectives, which reveals a convergent validity. In terms of internal consistency, the composite reliability (CR) was greater than 0.7 for all objectives, which reveals satisfactory construct reliability. To test the discriminant validity two criteria were used. First, the difference between the χ^2 values of the constrained and unconstrained model for each pair of objectives is statistically significant at 1% level. Second, the square root of AVE (Table 10 in bold) is higher than the correlation between objectives. We conclude that all the objectives show evidence of acceptable discrimination.

Table 10. Factor pattern for measures of mean objectives (n=221)

	Means	S.D.	C.R.	1	2	3	4	5
Maximize security of operational systems (1)	4.57	0.57	0.873	**0.797**				
Ensure buyer anonymity (2)	3.93	0.83	0.848	0.454***	**0.808**			
Minimize unwarranted solicitations (3)	3.46	0.90	0.808	0.246**	0.486***	**0.824**		
Understand the magnitude of customers' privacy fears (4)	2.50	1.39	0.897	-0.181*	0.047	0.342***	**0.902**	
Improve privacy guarantees (5)	4.69	0.60	0.843	0.725***	0.286***	0.188*	-0.211**	**0.854**

Likewise, for fundamental objectives, we first applied an exploratory factor analysis that revealed the same structure as was obtained in Phase 3. Next, we applied a confirmatory factor analysis. Again, the first objective revealed no sub-objectives with low loading but suggested several error correlations. The sub-objective *Emphasize the firms' reputation* and *Enhance company reputation* contains error correlation with the others sub-objectives, consequently we eliminated these sub-objectives. To establish unidimensionality for each objective, we analyzed objective in pairs to identify cross-loading. We eliminated the sub-objective *Emphasize respect for the firm* for cross loading reasons. We then re-tested the paired objectives to identify additional cross-loading. Next, we tested cross-loading in the full measured model and no cross loading was found. Then we tested the full measured model. As shown in Table 11, the final instrument for fundamental objectives has 5 objectives with 14 sub-objectives. The goodness-of-fit was checked with the respective cutoff as explained above. As we can see in Table 10, the goodness-of-fit indices for all measure are better than respective cutoffs. AVE was higher than the usual cutoff for all objectives, which reveals a convergent validity. In terms of internal consistency, the composite reliability (CR) was greater than 0.7 for all objectives, which reveals satisfactory construct reliability. To test the discriminant validity two criteria were used. First, the difference of χ^2 of constrained and χ^2 of unconstrained model for each pair of objectives is statistically significant at 1% level. This indicates discriminant validity. Second, with respect to the correlations between constructs and the square root of AVE, square root is higher than the correlation (Table 12 in bold). Based on these two criteria we conclude that the objectives show evidence of acceptable discrimination.

Table 11. Factor pattern for measures of fundamental objectives (n=221)

	Factor loading	Standard error	t-Value	R²
Maximize reputation of Internet Commerce vendor				
Emphasize trust in the retailer (FFO1_1)	0.904	-	-	0.82
Emphasize honesty of the retailer (FFO1_2)	0.896	0.035	27.6	0.80
Emphasize the integrity of the retailer (FFO1_3)	0.858	0.036	25.6	0.74
Emphasize trustworthiness of the site (FFO1_4)	0.668	0.040	16.7	0.45
Decrease spam				
Disallow spam (FFO2_1)	0.924	-	-	0.85
Disallow sending of spam after purchase (FFO2_2)	0.762	0.049	15.1	0.58
Decrease Spam (FFO2_3)	0.684	0.046	12.6	0.47
Maximize security of personal information				
Ensure Security of Personal Information (FFO3_1)	0.879	-	-	0.77
Ensure security of family info (FFO3_2)	0.762	0.067	12.7	0.58
Ensure confidentiality of personal info (FFO3_3)	0.615	0.059	11.0	0.38
Maximize privacy relative to online shopping				
Ensure privacy is consistent with speedy service (FFO4_1)	0.690	-	-	0.48
Ensure privacy is consistent with the efficiency of online shopping (FFO4_1)	0.949	0.143	8.1	0.90
Enhance shoppers' ability to control personal data				
Provide option to opt-out of lists (FFO5_1)	0.637	-	-	0.41
Provide the option not to be tracked (FFO5_2)	0.860	0.224	6.3	0.74
Goodness-of-fit indices:				
χ^2/d.f.= 1.69 (<3); TLI = 0.978 (>0.90); NFI = 0.962 (>0.90); CFI = 0.984 (>0.90); IFI = 0.984 (>0.90); GFI = 0.984 (>0.90); AGFI = 0.946 (>0.90); RMSEA = 0.039 (<0.07);				

Table 12. Factor pattern for measures of fundamental objectives (n=221)

	Means	S.D.	C.R.	1	2	3	4	5
Maximize reputation of Internet Commerce vendor (1)	4.07	0.75	0.902	**0.837**				
Decrease spam (2)	4.04	0.83	0.837	0.136**	**0.796**			
Maximize security of personal information (3)	4.57	0.62	0.800	0.252***	0.326***	**0.760**		
Maximize privacy relative to online shopping (4)	3.93	0.93	0.812	0.193***	0.225***	0.429***	**0.830**	
Enhance shoppers' ability to control personal data (5)	4.02	0.92	0.724	0.078	0.342***	0.341***	0.159**	**0.757**

The results of the data analysis provide evidence of reliability and construct validity for the 5 means objectives and the 5 fundamental objectives. The final instruments have good convergent validity, unidimensionality, construct reliability, and discriminant validity. The means and fundamental objectives instrument appears in Appendix A. Appendix B summarizes the means and fundamental objectives dimensions.

4. DISCUSSION AND IMPLICATIONS

Fear of loss of privacy in Internet Commerce is a genuine reaction of users who highly value individual privacy. Researchers study such reactions to the loss of privacy in terms of privacy concerns. Although, *concerns* provide an important insight into what causes perceptions of privacy loss, it certainly has a negative connotation. In this study, we adopt a more positive outlook to individuals who value their privacy and define objectives for the institutionalization of their privacy protection. To this effect, building on Keeney (1994), this study perceives privacy in Internet Commerce as an opportunity, rather than a problem. As Keeney notes:

> "Decision makers usually think of decision situations as problems to be solved, not as opportunities to be taken advantage of. It is perhaps not surprising that decision makers do not systematically hunt for decision situations. Who needs yet another problem? …recognizing and following up on decision opportunities is analogous to prevention, whereas dealing with decision problems is analogous to cure." (p. 241)

From a privacy perspective, such an opportunistic view could alleviate some decision problems or avoid many future problems. Indeed, ensuring individual privacy in Internet Commerce presents a strategic decision opportunity to change to a more advantageous context. However, as Keeney questions, "How many individuals or organizations have written down their strategic objectives? How many have even carefully thought about them?" (p. 242). The elusive and problematic nature of privacy in Internet Commerce is an evidence that little effort is made to recognize and operationalize privacy as an opportunity. The challenge is to develop procedures that will on the one hand help organizations gain intelligence from such information, and on the other hand will protect the interests of customers in terms of privacy. Such balanced procedures clearly require the quantification or prioritization of means and fundamental objectives. For individuals and organizations, the evaluation of objectives itself present a decision situation. Considering the tradeoffs among different objectives and the risk attitude of strategic decision makers, one could quantify or prioritize such objectives, using a utility function of the form $u(x)=u(x_1,x_2,\ldots,x_n)$, where u(x) represent the utility of overall strategic objective x_1, x_2, and x_n represents the utility of each fundamental or mean objective.

4.1. Theoretical Implications

There are several theoretical implications of this study. First, the factor model for fundamental and mean objectives is grounded in individual values. Previous research uses privacy concerns or responses to those concerns as proxy for privacy; such observations have been made by other scholars as well (see, Bélanger & Crossler, 2011; Dinev, et al., 2013; Malhotra, et al., 2004; Pavlou, 2011; Smith, et al., 1996; Stewart & Segars, 2002). In comparison, values, in normative agreement, are moral beliefs which people lean on for the rationale of their actions (Spates, 1983). Therefore, privacy concerns and responses are actions that people take to appeal to the protection of their privacy.

Second, by adopting Kenney's view of objectifying the values, means and fundamental objectives provide an actionable strategy for ensuring information privacy. Previous research that studies privacy concerns and responses assumes privacy as being a "problem", and hunts for its "cure" ("problem" and "cure" are terms used by Keeney (1992). Furthermore, none of the existing studies provide strategies for overcoming such concerns. However, privacy really is not a "concern", but an opportunity. Our study is the first of its type to accept privacy as a strategic decision opportunity. By following a strategic decision analysis perspective, the values are converted to objectives, whereby the objectives focus on "prevention."

Third, the exploratory nature of this research allowed us to question **what** values users attribute to their individual privacy and how such values can be preserved. In particular, the proposed objectives are derived from user values. Thus, our study switches the focus from normative to exploratory or descriptive findings (Bélanger & Crossler, 2011; Smith, et al., 2011). The four-large scale empirical studies allowed us to develop a more reliable and a valid instrument to measure the institutionalization of individual privacy in Internet Commerce. The research design allowed us to overcome the shortcoming that much of the existing conceptualization of privacy suffers from (see, Bélanger & Crossler, 2011; Dinev, et al., 2013; Pavlou, 2002). Moreover, the sequential mixed method-based design also allowed us to leverage the benefits of both qualitative and quantitate methodologies. While the qualitative nature of the research design focuses on developing initial set of objectives from individual values about information privacy in Internet Commerce, multiple quantitative studies validated the objectives and increased their generalizability. In order to fully understand the values of individual privacy, we conceptualized individual privacy within the context of Internet Commerce and thus heeded to calls made by previous researchers (see, Malhotra, et al., 2004; Solove, 2002).

Finally, the sequential and multiple confirmatory studies allowed for a validated and rigorous synthesis of objectives. The fundamental objectives are certainly essential to guide any strategic planning initiative for managing individual privacy in an Internet Commerce environment, and the means of achieving those fundamental objectives are equally important. The meaning of many of the means and fundamental objectives are obvious; however, some elaboration is appropriate.

Interestingly, among the fundamental objectives, "maximize reputation of Internet Commerce vendor" has been well researched, albeit in the context of a consumer willingness to purchase online. Various researchers have noted the reasons that affect an individual's intention to trust a vendor. Among many reasons such as trusting attitude, past experience, perceived risk, and website quality, corroborate with our findings (see, Einwiller, 2003; McKnight, Choudhury, & Kacmar, 2002). However, with respect to individual privacy protection, vendor trust has largely been considered as a surrogate measure. Luo (2002), for instance, proposes several trust building mechanisms which in turn decrease privacy concerns: community feeling, repeated purchases, digital certificates. Our research also identifies several objectives, which come together to enhance the reputation of an Internet vendor, the lack of which elevates consumer fears about their privacy.

Another important fundamental objective in ensuring individual privacy is "decrease spam". In the extant literature, unsolicited marketing emails are regarded as spam and given that an email uses customer's personal information, such solicitations are considered privacy violations (Mai, et al., 2010). While existing studies consider security and privacy as a "panacea against identity theft and spam" (p. 8 Teltzrow & Kobsa, 2004), our research indicates that ensuring information privacy *ex post* is critical for a long term *business to customer* relationship. For example, one of the sub-objectives identified is, "disallow sending of spam after purchase". When we traced the origin of this objective back to the interviews conducted in Phase 1, we found a respondent stating the following:

> "Online privacy is not so much about limiting email blasts from vendors that you don't know, but it is more about solicited and unsolicited emails and promotional materials that one receives from vendors with whom you engage in a transaction. For instance, a long time ago I purchased something from talbots.com. Now I have been receiving almost a message a day. Not that I care, but it bothers me when I have to pay roaming charges internationally to download emails. I also dare not go and undo subscribe options, particularly when one cannot trust these sites… remember what happened with DSW."

While our objectives certainly discourage spam, it might be interesting to further investigate the relationship between spam and privacy following a purchase. Our remaining three fundamental objectives – *maximize security of personal information*, *maximize privacy relative to online shopping* and *enhance shopper's ability to control personal data* – suggest that users are concerned about the moral hazards (Pavlou, Liang, & Xue, 2007). Our objectives echo the findings of Kobsa (2001) who presented a three tier classification of personal information: (1) *User data* refers to personal characteristic of a user; (2) *Usage data* refers to a user's interactive behavior with the system, and; (3) E*nvironment data* refers to the locale of the user. Thus, with the intention of optimal information privacy, consumers need to know **what** customer data is collected, **how** the data is used and **where** the data resides. The intention is succinctly captured in the following words of one the interviewees:

> "I need to know what personal information they want to collect and where it will reside. Ideally, I don't want it to reside anywhere. I also want to know how quickly my request can be processed. Most businesses today seem to collect a lot of personal information under the guise of providing efficient services. That is not true. Finally, I also want to

> know if I can safely delete the information. Usually opting out of a mailing list may not result in deletion of your data."

Our research found that *security of operational systems*, *buyer anonymity*, *unwarranted solicitations*, *understanding magnitude of customer fears* and *enhancing privacy guarantees* will foster an environment that ensures responsible privacy practices. These means objectives hark back to some basic principles, which have unfortunately been forgotten as the dependence on ecommerce increased. As one of one respondents notes:

> "E-commerce has complicated things for us. 30 years ago I could walk in to a corner store, buy what I want to, pay cash and walk away. Today in the e-commerce domain, I have to register myself in a shop, leave my home contact details with them … just so that I can buy something. This seems ridiculous. Rather than displaying specials in a window of a shop, retailers force their publicity down my throat and at times even want me to pay for their publicity. Something is really wrong here."

4.2. Practical Implications

In this paper we have rigorously developed the value based fundamental objectives and the means to achieve them. The methodology used has been well accepted in the literature. The objectives provide a useful basis on a number of fronts:

1) The fundamental objectives are a generic set of strategic objectives that any Internet Commerce organization needs to be aware of in addressing information privacy. For instance, Internet Commerce vendors need to ensure that they maintain a high level of reputation. Failure to do so will result in loss of consumer trust. Similarly, decreasing spam, ensuring security of personal information, providing an ability to the

consumers to control personal data and generally ensure privacy are all fundamental to a successful information privacy objective[5]. Our research systematically identified these objectives based on a well-established value-focused approach. Our research also provides several means to achieve the fundamental objectives, which are measures that can be used by other researchers.

2) Organizations can also systematically evaluate how well they are performing relative to the fundamental and means objectives. In that sense, findings from our research form a basis for an organizational self-assessment of information privacy practices. While the objectives do not necessarily prescribe a particular approach, for example, reduce spam or give ability to control personal data, the generic direction is indeed spelled out.

3) Given that our research uses an individual value-based perspective, consumers can themselves use the objectives as a self-evaluation guide to judge if a given Internet Commerce business adheres to, or seriously considers privacy. Although in many cases this may result in a consumer still transacting business with the given Internet Commerce company, it may in some cases influence consumers otherwise. We consider this benefit to be of secondary importance though.

4.3. Limitations and Future Research Directions

[5] As we prepared the revision of this paper, the Campbridge Analytica and Facebook breach came to light. On April 5, 2018, Mark Zucherberg admitted that mistakes related to privacy had been made. Interestingly, all our fundamental objectives were relevant and central to the argumentation. See https://www.cnbc.com/2018/04/04/mark-zuckerberg-facebook-user-privacy-issues-my-mistake.html

This study has some limitations which leads to future research directions. The objectives were defined from the values of graduate students in a university. Although, the selection criteria ensured that the participants have a fair knowledge of privacy in the context of Internet Commerce sites, the objectives do not reflect the values of non-users. Hence future research can adopt a more inclusive approach in selecting the participants for value elicitation.

The final set of objectives established a valid and useful basis for the ongoing assessment of privacy concerns and policies. One interesting avenue is to determine the relative importance of the objectives in achieving strategic information privacy. This study proposes five-factor means objectives and five-factor fundamental objectives model for ensuring individual privacy derived from a series of studies and thus increasing validity and reliability of factors. However, future research needs to determine the relative significance of these objectives in ensuring privacy. To this end, a prediction model for individual privacy as a function of these objectives could be developed.

Based on decision analysis, the objectives present an opportunity to strategize about ensuring privacy. As such, a responsible decision maker has to balance the consequences of uncertain outcomes with respect to the preferred outcomes (Keeney, 1994). By assigning the probabilities and utilities to the consequences, the decision maker can calculate an optimal strategy to maximize the expected utility of Internet Commerce. Another possible avenue is to determine changes that an institutionalization of these objectives will require. For example, it would be interesting to examine the impact of these objectives on the existing policies or infrastructure. Finally, as many scholars recognize the importance of contextualizing privacy (see, Culnan, 1993; Malhotra, et al., 2004; Solove, 2006), the objectives could be evaluated in other technical contexts such as social media.

5. CONCLUSION

Privacy in Internet Commerce has turned out to be elusive and problematic. Users are perplexed whether to share or withhold their personal information for leveraging the benefits of Internet Commerce. To this effect, an epistemic question calls for attention: what values users attribute to individual privacy and how protection can be established. The main purpose of this study was to advance the theoretical understanding of individual privacy in an Internet Commerce environment. To this effect, this research adopted a value-based view of privacy to better understand the values that users attribute to privacy in Internet Commerce. A sequential mixed methods approach was employed to empirically explore and validate a parsimonious set of means and fundamental objectives that are grounded in the values of Internet Commerce users. Together, the objectives form the basis for ensuring individual privacy. The rigorous approach that was used to develop the objectives sets these objectives as being validated and generalizable, thus forming a basis for future research. Such an understanding would allow organizations and individuals to strategize about individual privacy. The objectives could also prove useful for policy makers to assure consumer privacy.

References

Allen, J.P. (2005). Value conflicts in enterprise systems. *Information Technology & People,* 18(1), 33-49.

Anderson, J.C. (1987). An approach for confirmatory measurement and structural equation modeling of organizational properties. *Management Science,* 33(4), 525-541.

Anderson, J.C., & Gerbing, D.W. (1988). Structural equation modeling in practice: A review and recommended two-step approach. *Psychological Bulletin,* 103(3), 411-423.

Awad, N.F., & Krishnan, M. (2006). The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly,* 30(1), 13-28.

Awang, Z. (2012). *Structural equation modeling using AMOS graphic*: Penerbit Universiti Teknologi MARA.

Baier, K. (1990). Egoism. In P. Singer (Ed.), *A Companion to Ethics*: Wiley-Blackwell.

Baumgartner, H., & Homburg, C. (1996). Applications of structural equation modeling in marketing and consumer research: A review. *International journal of Research in Marketing,* 13(2), 139-161.

Bélanger, F., & Crossler, R.E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS quarterly,* 35(4), 1017-1042.

Bollen, K.A. (1989). *Structural equations with latent variables*. New York: Wiley.

Boudreau, M.-C., Gefen, D., & Straub, D.W. (2001). Validation in information systems research: A state-of-the-art assessment. *MIS Quarterly*, 1-16.

Brown, T.A. (2014). *Confirmatory factor analysis for applied research*: Guilford Publications.

Browne, M.W. (1968). A comparison of factor analytic techniques. *Psychometrika,* 33(3), 267-334.

Buchanan, T., Paine, C., Joinson, A.N., & Reips, U.D. (2007). Development of measures of online privacy concern and protection for use on the Internet. *Journal of the Association for Information Science and Technology,* 58(2), 157-165.

Campbell, D.T., & Fiske, D.W. (1959). Convergent and discriminant validation by the multitrait-multimethod matrix. *Psychological Bulletin,* 56(2), 81-105.

Cattell, R. (2012). *The scientific use of factor analysis in behavioral and life sciences*: Springer Science & Business Media.

Chang, J.C.-J., Torkzadeh, G., & Dhillon, G. (2004). Re-examining the measurement models of success for Internet commerce. *Information & Management,* 41(5), 577-584.

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

Chen, S.C., & Dhillon, G.S. (2003). Interpreting dimensions of consumer trust in e-commerce. *Information Technology and Management,* 4(2-3), 303-318.

Churchill, G.A. (1979). A paradigm for developing better measures of marketing constructs. *Journal of Marketing Research,* 16(1), 64-73.

Connor, P.E., & Becker, B.W. (1975). Values and the organization: Suggestions for research. *Academy of Management Journal,* 18(3), 550-561.

Culnan, M.J. (1993). "How did they get my name?": An exploratory investigation of consumer attitudes toward secondary information use. *MIS Quarterly*, 341-363.

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

Culnan, M.J., & Williams, C.C. (2009). How ethics can enhance organizational privacy: Lessons from the ChoicePoint and TJX data breaches. *MIS Quarterly,* 33(4), 673-687.

Dhillon, G., Oliveira, T., Susarapu, S., & Caldeira, M. (2016). Deciding between information security and usability: Developing value based objectives. *Computers in Human Behavior,* 61, 656-666.

Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. *Information Systems Journal,* 16(3), 293-314.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research,* 17(1), 61-80.

Dinev, T., Xu, H., Smith, J.H., & Hart, P. (2013). Information privacy and correlates: An empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems,* 22(3), 295-316.

Doll, W.J., & Torkzadeh, G. (1988). The measurement of end-user computing satisfaction. *MIS Quarterly,* 12(2), 259-274.

Dwoskin, E. (2014). Give me back my online privacy. In *Wall Street Journal. March 24 (available at http://www.wsj.com)*.

Einwiller, S. (2003). When reputation engenders trust: An empirical investigation in business-to-consumer. *Electronic Markets,* 13(3), 196-209.

Everitt, B. (1975). Multivariate analysis: The need for data, and other problems. *The British Journal of Psychiatry,* 126(3), 237-240.

Feinberg, J. (2007). Psychological egoism. In R. Shafer-Landau (Ed.), *Ethical Theory: An Anthology* (pp. 183): Wiley-Blackwell.

Fornell, C., & Larcker, D.F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, 39-50.

Forza, C., & Filippini, R. (1998). TQM impact on quality conformance and customer satisfaction: a causal model. *International journal of production economics,* 55(1), 1-20.

Friedman, B., Kahn Jr, P.H., & Borning, A. (2006). Value sensitive design and information systems. In P. Zhang & D. Galletta (Eds.), *Human-computer interaction in management information systems: Foundations*

Gregory, R., & Keeney, R.L. (1994). Creating policy alternatives using stakeholder values. *Management Science,* 40(8), 1035-1048.

Hair, J.F. (2010). *Multivariate Data Analysis: A Global Perspective*: Pearson Education.

Hair, J.F., Black, W.C., Babin, B.J., Anderson, R.E., & Tatham, R.L. (2010). *Multivariate data analysis (7th ed.)* (Vol. 5). Upper Saddle River, NJ: Prentice hall, Inc.

Hedström, K., Kolkowska, E., Karlsson, F., & Allen, J. (2011). Value conflicts for information security management. *The Journal of Strategic Information Systems,* 20(4), 373-384.

Hemingway, C.A., & Maclagan, P.W. (2004). Managers' personal values as drivers of corporate social responsibility. *Journal of Business Ethics,* 50(1), 33-44.

Hofstra, B., Corten, R., & van Tubergen, F. (2016). Understanding the privacy behavior of adolescents on Facebook: The role of peers, popularity and trust. *Computers in Human Behavior,* 60, 611-621.

Homer, P.M., & Kahle, L.R. (1988). A structural equation test of the value-attitude-behavior hierarchy. *Journal of Personality and Social Psychology,* 54(4), 638-646.

Keeney, R.L. (1992). *Value-focused thinking: a path to creative decisionmaking*. Cambridge, Massachusetts: Harvard University Press.

Keeney, R.L. (1994). Creativity in decision making with value-focused thinking. *Sloan Management Review,* 35(4), 33-33.

Keeney, R.L. (1999). The value of Internet commerce to the customer. *Management Science,* 45(4), 533-542.

Kerlinger, F.N. (1978). *Foundations of Behavioral Research* New York: McGraw-Hill.

Kim, D.J. (2008). Self-perception-based versus transference-based trust determinants in computer-mediated transactions: A cross-cultural comparison study. *Journal of Management Information Systems,* 24(4), 13-45.

Kline, R. (2005). Principles and Practice of Structural Equation Modeling (2nd Edition ed.). In. New York: Guilford Press.

Kling, R. (1978). Value conflicts and social choice in electronic funds transfer system developments. *Communications of the ACM,* 21(8), 642-657.

Kling, R. (1980). Social analyses of computing: Theoretical perspectives in recent empirical research. *ACM Computing Surveys,* 12(1), 61-110.

Kobsa, A. (2001). Generic user modeling systems. *User modeling and user-adapted interaction,* 11(1-2), 49-63.

Lee, D.-J., Ahn, J.-H., & Bang, Y. (2011). Managing consumer privacy concerns in personalization: A strategic analysis of privacy protection. *MIS Quarterly,* 35(2), 423-444.

Li, T., & Unger, T. (2012). Willing to pay for quality personalization? Trade-off between quality and privacy. *European Journal of Information Systems,* 21(6), 621-642.

Luo, X.M. (2002). Trust production and privacy concerns on the Internet - A framework based on relationship marketing and social exchange theory. *Industrial Marketing Management,* 31(2), 111-118.

MacCallum, R.C., Widaman, K.F., Zhang, S., & Hong, S. (1999). Sample size in factor analysis. *Psychological methods,* 4(1), 84.

Mai, B., Menon, N.M., & Sarkar, S. (2010). No free lunch: Price premium for privacy seal-bearing vendors. *Journal of Management Information Systems,* 27(2), 189-212.

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,* 15(4), 336-355.

Mallat, N. (2007). Exploring consumer adoption of mobile payments–A qualitative study. *The Journal of Strategic Information Systems,* 16(4), 413-432.

May, J., Dhillon, G., & Caldeira, M. (2013). Defining value-based objectives for ERP systems planning. *Decision Support Systems,* 55(1), 98-109.

McDaniels, T., & Trousdale, W. (1999). Value-focused thinking in a difficult context: planning tourism for Guimaras, Philippines. *Interfaces,* 29(4), 58-70.

McKnight, D.H., Choudhury, V., & Kacmar, C. (2002). The impact of initial consumer trust on intentions to transact with a web site: A trust building model. *The Journal of Strategic Information Systems,* 11(3), 297-323.

Moores, T.T., & Dhillon, G. (2003). Do privacy seals in e-commerce really work? *Communications of the ACM,* 46(12), 265-271.

Nunnally, J. (1978). Psychometric theory. In: New York: McGraw-Hill.

Parsons, K., Calic, D., & Barca, C. (2016). Self-Disclosure on Facebook: Comparing two Research Organisations. The 27th Australasian Conference on Information Systems, 5-7 December, Wollongong.

Pavlou, P.A. (2002). Institution-based trust in interorganizational exchange relationships: The role of online B2B marketplaces on trust formation. *The Journal of Strategic Information Systems,* 11(3), 215-243.

Pavlou, P.A. (2011). State of the information privacy literature: Where are we now and where should we go. *MIS Quarterly,* 35(4), 977-988.

Pavlou, P.A., Liang, H., & Xue, Y. (2007). Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *MIS Quarterly,* 31(1), 105-136.

Segars, A.H. (1997). Assessing the unidimensionality of measurement: a paradigm and illustration within the context of information systems research. *Omega,* 25(1), 107-121.

Segars, A.H., & Grover, V. (1993). Re-examining perceived ease of use and usefulness: A confirmatory factor analysis. *MIS Quarterly,* 17(4), 517-525.

Segars, A.H., & Grover, V. (1998). Strategic information systems planning success: an investigation of the construct and its measurement. *MIS Quarterly,* 22(2), 139-163.

Shankar, V., Urban, G.L., & Sultan, F. (2002). Online trust: a stakeholder perspective, concepts, implications, and future directions. *The Journal of Strategic Information Systems,* 11(3), 325-344.

Sheng, H., Nah, F.F.-H., & Siau, K. (2005). Strategic implications of mobile technology: A case study using Value-Focused Thinking. *The Journal of Strategic Information Systems,* 14(3), 269-290.

Smith, H.J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly,* 35(4), 989-1016.

Smith, H.J., Milberg, S.J., & Burke, S.J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS quarterly,* 20(2), 167-196.

Solove, D.J. (2002). Conceptualizing privacy. *California Law Review*, 1087-1155.

Solove, D.J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, 477-564.

Spates, J.L. (1983). The sociology of values. *Annual Review of Sociology*, 27-49.

Steiger, J.H. (2007). Understanding the limitations of global fit assessment in structural equation modeling. *Personality and Individual differences,* 42(5), 893-898.

Stewart, K.A., & Segars, A.H. (2002). An empirical examination of the concern for information privacy instrument. *Information Systems Research,* 13(1), 36-49.

Tan, F.B., & Hunter, M.G. (2002). The repertory grid technique: A method for the study of cognition in information systems. *MIS Quarterly,* 26(1), 39-57.

Tang, Z., Hu, Y., & Smith, M.D. (2008). Gaining trust through online privacy protection: Self-regulation, mandatory standards, or caveat emptor. *Journal of Management Information Systems,* 24(4), 153-173.

Teltzrow, M., & Kobsa, A. (2004). Impacts of user privacy preferences on personalized systems. In C.M. Karat, J.O. Blom & J. Karat (Eds.), *Designing personalized user experiences in eCommerce* (pp. 315-332): Springer.

Torkzadeh, G., & Dhillon, G. (2002). Measuring factors that influence the success of Internet commerce. *Information Systems Research,* 13(2), 187-204.

Tsai, J.Y., Egelman, S., Cranor, L., & Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research,* 22(2), 254-268.

Turban, E., Outland, J., King, D., Lee, J.K., Liang, T.-P., & Turban, D.C. (2018). E-Commerce: Regulatory, Ethical, and Social Environments. In *Electronic Commerce 2018* (pp. 573-612): Springer.

Venkatesh, V., Brown, S.A., & Bala, H. (2013). Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. *MIS Quarterly,* 37(1), 21-54.

Wattal, S., Telang, R., Mukhopadhyay, T., & Boatwright, P. (2012). What's in a “name”? Impact of use of customer information in e-mail advertisements. *Information Systems Research,* 23(3-part-1), 679-697.

Weiss, D.J. (1970). Factor analysis and counseling research. *Journal of Counseling Psychology,* 17(5), 477.

Appendix A – Instrument for assessing means and fundamental objectives

Below you will find a series of questions that will assess your attitudes about how important Internet privacy is to you when you are buying items online. Using the range of response options provided - i.e., your response selections can range from 1 (strongly disagree) to 5 (strongly agree). There are no right or wrong answers; just try to answer as honestly as you can.

Means and Fundamental Objectives about individual information privacy in Internet commerce

To ensure Internet privacy, it is important to:	1 – Strongly disagree	2	3	4	5 – Strongly agree
Decrease Spam					
Disallow sending of spam after purchase					
Disallow solicitations from salespeople					
Disallow spam					
Disallow use of direct marketing					
Downplay privacy fears					
Emphasize honesty of the retailer					
Emphasize the integrity of the retailer					
Emphasize trust in the retailer					
Emphasize trustworthiness of the site					
Ensure Buyer Anonymity					
Ensure confidentiality of personal info					
Ensure privacy is consistent with speedy service					
Ensure privacy is consistent with the efficiency of online shopping					
Ensure security of family info					
Ensure Security of Personal Information					
Maximize protection of financial information					
Maximize security after the transaction					
Maximize security of website					
Maximize shopper anonymity					
Maximize transaction security					
Maximize web surfer anonymity					
Minimize importance of privacy					
Provide guarantees of secure transactions					
Provide option to opt-out of lists					
Provide privacy guarantees					
Provide the option not to be tracked					

Appendix B – Means and fundamental objectives dimensions

Means objectives	**Fundamental objectives**
Maximize security of operational systems	**Maximize reputation of Internet Commerce vendor**
Maximize security after the transaction	Emphasize trust in the retailer
Maximize transaction security	Emphasize honesty of the retailer
Maximize security of website	Emphasize the integrity of the retailer
Maximize protection of financial information	Emphasize trustworthiness of the site
Ensure buyer anonymity	**Decrease spam**
Maximize shopper anonymity	Disallow spam
Maximize web surfer anonymity	Disallow sending of spam after purchase
Ensure Buyer Anonymity	Decrease Spam
Minimize unwarranted solicitations	**Maximize security of personal information**
Disallow use of direct marketing	Ensure Security of Personal Information
Disallow solicitations from salespeople	Ensure security of family info
	Ensure confidentiality of personal info
Understand the magnitude of customers' privacy fears	
Minimize importance of privacy	**Maximize privacy relative to online shopping**
Downplay privacy fears	Ensure privacy is consistent with speedy service
	Ensure privacy is consistent with the efficiency of online shopping
Improve privacy guarantees	
Provide guarantees of secure transactions	**Enhance shoppers' ability to control personal data**
Provide privacy guarantees	Provide option to opt-out of lists
	Provide the option not to be tracked

- Objectives to ensure information privacy of Internet Commerce users are identified
- Research presents a measurement scale, which is useful for researchers and marketers
- Scale measures how customer attitudes about privacy influence Internet behavior
- A sequential mixed-methods approach to measure institutionalization of privacy