PRIVACY PARADOX: DOES STATED PRIVACY CONCERNS TRANSLATE INTO THE VALUATION OF PERSONAL INFORMATION?

Luvai F. Motiwalla  
*University of Massachusetts Lowell, luvai_motiwalla@uml.edu*

Xiaobai (Bob) Li  
*University of Massachusetts Lowell, xiaobai_li@uml.edu*

Xiaoping Liu  
*University of Massachusetts Lowell, xiaoping_liu@student.uml.edu*

Follow this and additional works at: [http://aisel.aisnet.org/pacis2014](http://aisel.aisnet.org/pacis2014)
PRIVACY PARADOX: DOES STATED PRIVACY CONCERNS TRANSLATE INTO THE VALUATION OF PERSONAL INFORMATION?

Luvai F. Motiwalla, Department of OIS, University of Massachusetts Lowell, USA, luvai_motiwalla@uml.edu
Xiaobai (Bob) Li, Department of OIS, University of Massachusetts Lowell, USA, xiaobai_li@uml.edu
Xiaoping Liu, Department of OIS, University of Massachusetts Lowell, USA, xiaoping_liu@student.uml.edu

Abstract

Information privacy paradox is of great interest to IS researchers and firms gathering personal information. This paradox has been found by IS researchers from social, behavioral, and economic aspects independently. However, there is a lack of study that examines the degrees of influence that different factors contribute to the privacy paradox problem. We combine both economic and social perspectives in our study of the privacy paradox with an economic valuation of personal information through an auction experiment in first market exchange combined with a behavioral study on general privacy concerns and specific disclosure behaviors. Our goal is to reveal more insights on the paradox through a privacy auction on personal information. Results indicate that individuals’ privacy concerns do not have a significant influence on their valuations of personal information. Instead, their prior disclosure behaviors in specific situations, like with health-care providers or social networks, are better indicators of their valuations.

Keywords: Privacy paradox, privacy concerns, disclosure behaviors, privacy calculus, personal information, price valuation
1. INTRODUCTION

The success of business intelligence increasingly depends on the effective analysis of customer data (Culnan & Armstrong 1999). Many online businesses have been collecting consumer information in a secondary exchange (Culnan & Bies 2003) for some economic or social benefit, either through personalization incentives or from loyalty programs (Krohn et al. 2002). Today, privacy is often considered as a currency through which we pay for free access to web content and get discounts on all sorts of retail products and services; therefore, consumers today want to know what benefits they can get in return for sharing their information (Mitchell 2013). Secondary data is nowadays traded among service providers like other commodities, meriting an analysis of individual transactions in the marketplace. According to Jenitzsch et al. (2012), 47% of the service providers treated customer data as a commercial asset; and 48% revealed that they share data with third parties. The recent spike in data snooping, however, has heightened consumer privacy concerns and industry regulations, making the online commerce environment complex and expensive. Financial or health-care services, which can use information technology to become more personalized, efficient and cost competitive, are impeded due to consumer privacy concerns. Therefore, it is important to understand both social and economic dimensions of information privacy.

Research communities have tried to understand information privacy concerns in an effort to improve online commerce. Information privacy concerns surface when consumers perceive information collection and sharing procedures as an invasion of privacy (Zhou 2012). For example, the National Security Agency (NSA) of the US has been collecting phone and other records on all Americans. This revelation has increased privacy concerns of all individuals (Gage 2013). Individuals in western society often see privacy as a control and a rights issue. Information privacy can be defined as the right of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others (Westin 1967). Overcoming these privacy concerns is a popular issue in today’s digital economy, because digital profiling can remotely and secretly collect significant amounts of personal information that can be stored indefinitely (Adomavicius & Tuzhilin 2005). Smith et al. (1996) and Malhotra et al. (2004) have identified consumer concern factors related to privacy practices and developed survey instruments to measure users’ information privacy concerns such as data collection procedures, control, and awareness of privacy practices. Similarly, Lwin et al. (2007) have used a power–responsibility equilibrium framework to examine the antecedents and consequences of information privacy concerns. They found consumers adjust their privacy defenses when data protection policy is ill-defined and information requested by firms is incongruent of the interaction contexts. Namely, consumers adjust their behaviors when information requested is of sensitive nature and not relevant for the execution of transaction.

This study contributes to existing research on information privacy (Smith et al. 1996; Culnan & Bies 2003; Dinev & Hart 2006) which states that most consumers conduct risks and benefits calculus before disclosing their personal information to an organization. Risk factors include data collection methods, secondary usage, error, access, control and awareness (Hong & Thong 2013). Benefit factors typically include personalization, financial rewards and social adjustments (Smith et al. 2011). Another consideration that consumers often include in their privacy calculus is trust (Van Slyke et al. 2006; Norberg et al. 2007), which is influenced by the firms’ reputation and observation of its privacy policy and culture for data protection (Buchanan et. al. 2007). Our contribution is in exploring relationships between consumers’ privacy concerns and disclosure behaviors, and their actual price valuations of personal information in a single utilitarian exchange (Bogozzi 1975); i.e., first exchange where goods and services are exchanged for money (Culnan & Milberg 1998). Previous studies in information privacy have examined consumer behavior in secondary exchange (Culnan & Bies 2003) where consumers trade their personal information for non-monetary social values such as future promises or benefits (Milne & Gordon 1993). This social exchange perspective has focused on consumers’ willingness to disclose information (Dinev & Hart 2006), willingness to pay for premium services (Schreiner et al. 2012), or willingness to share for personalization benefits (Awad & Krishnan 2006) as a proxy for price valuation for personal information. Social exchanges have been complimented with experimental economic exchanges in some studies. Jensen et al. (2005),
Huberman et al. (2005), Chellappa & Sen (2007), John et al. (2010), Tsai et al. (2011) have all conducted various forms of economic experiments to complement their survey findings to observe users’ behavior on privacy. Yet, they have not specifically investigated the relationship among privacy concerns, behaviors and price value of information in a first exchange, where consumers can trade their personal data in exchange for a price.

Our research study investigates the relationship between individuals’ privacy concerns and disclosure behaviors on their privacy valuations in a first or primary exchange. It combines the social and economic perspectives by looking at the actual disclosure behavior of consumers in an economic exchange experiment, where 218 participants were asked to bid in dollar amounts for selling their personal information in an auction, followed by a survey on consumers’ general privacy concerns, personal disclosure risks, and disclosure behaviors. Preliminary results indicate that general privacy concerns and personal disclosure risks are poor indicators of consumers’ price valuations for their personal information. On the other hand, we find that consumer’s prior disclosure behaviors -- such as sharing personal data with physicians, family members or friends and in social media (Facebook) -- have a significant relationship on their price valuations.

The rest of the paper is organized as follows. The next section reviews the relevant privacy literature and its limitation in understanding the actual economic valuation of personal information. The third section presents our research model and hypothesis, followed by the fourth section which presents our methodology and data analysis. The final section concludes with a discussion on our findings, limitations and future research directions.

2. LITERATURE REVIEW

The privacy literature offers several theories on the relationship between consumers’ information privacy concerns and their willingness to disclose personal information. The first studies on general privacy concerns emerged in late 1960s (Westin 1967). Westin’s main focus was on individual privacy rights and control over information collected by organizations based on individuals’ perceptions of distrust and fears of abuse with information technology (Westin 2000). The Westin-Harris consumer privacy surveys from the late 1970s until the 2004 have focused on several privacy domains from general privacy concerns to more focused areas in marketing, medical, and online commerce (Kumaragur & Cranor 2005), which have resulted in a methodical privacy index that segments individuals into three categories known as privacy fundamentalist, pragmatist and unconcerned (Harris et al. 1991). The Westin-Harris privacy indexes are useful indicators of the consumers’ privacy concerns and attitudes as measured by the thousands of US consumers over a long period of time, and these survey questions have been validated by other privacy concern studies (Carlos 2005). However, these surveys and their resulting segments do not provide information on how individual information disclosure decisions are affected by privacy concerns or how individuals’ attest economic value on their personal data.

This limitation has led to research that focuses on individual disclosure decisions under risk uncertainty (Kahnemann & Trevesky 1984). With the large scale growth in the Web and electronic commerce in the 1990s, privacy researchers were interested in consumer behaviors on remote data collection through Web technologies like anonymous cookies for personalization services (Culnan & Bies 2003; Krohn et al. 2008) and sharing of this personal information with other firms (Winer 2001). From this research there emerged a consensus that consumers can experience both benefits and risks when disclosing their personal information (Culnan & Bies 2003). Based on social exchange perspective, Laufer and Wolfie (1977) investigated individual disclosure behavior of consumers and found that they were willing to disclose their personal information provided it was not abused by the firm and did not have negative consequences on their privacy. This cost-benefit calculus was analyzed through a secondary exchange which focuses on the social and long-term benefits of secondary uses of data and coined the term privacy calculus (Culnan & Bies 2003).

Several researchers have focused on this privacy calculus model to analyze user privacy behavior in the last decade (Belanger & Crossler 2011; Smith et al. 2011). The simplicity of this model has allowed researchers to group consumers’ risk beliefs and attitudes into cost factor and contrasts them...
with both tangible and intangible rewards into the benefits factor, and to understand its influence on their willingness to disclose personal information. Risk measures include consumer attitudes towards data collection, storage protection, accuracy and control policies of the firms through concern for information privacy survey (Smith et al. 1996) construct and internet users concerns for information privacy construct (Malhotra et al., 2004). Similarly, consumers’ benefits are captured either through surveys or observations during online commerce experimental studies. These benefits are grouped into personalization, loyalty rewards or financial rewards (Wilson & Valachich 2012). Trust, based on a firms’ reputation with fair information practices, was another factor included in many of these studies, either as part of benefits or separately to measure its influence on risk in the consumers’ privacy calculus equations (Mayer et al. 1995).

The privacy calculus studies address the limitation of Westin-Harris studies because they provide additional details on consumers’ decision making process under risk uncertainty of disclosing personal information and provide firms with measures to collect personal information with incentives. Privacy calculus has been considered as a useful framework (Laufer & Wolfe 1977; Culnan & Bies 2003; Smith et al. 2011; Dinev & Hart, 2006) to study consumer behavior in a privacy exchange. Privacy calculus basically states that consumers generally perform a risk-benefit analysis before data disclosure or sharing decisions. They analyze the risks of disclosing their personal data in relation to the benefits achieved from this disclosure. Risk has been defined in this context of an individual’s willingness to share information despite the negative consequences such as marketing messages, health-care coverage and others. Individuals’ perceptions on privacy concerns as well as trust often change as they often calculate risks and benefits differently over a period of time (Acquisti 2004), yet the calculus trade-off is an important research issue to be considered in privacy (Pavlou 2011). However, several studies that focused on the calculus model found that while consumers’ are highly concerned about privacy risks their information disclosure behaviors in actual information sharing situations are often inconsistent with their stated privacy concerns. This has led a number of follow-up studies on privacy paradox.

Privacy paradox research (Acquisti & Grossklas 2005; Hann et al. 2007; Tsai et al. 2011; Keith, et al. 2013) finds consumers’ actions (actual behaviors) during privacy transactions contradict with their concerns on privacy risks when disclosing personal information in exchange for rewards (Noorberg et al. 2007). While consumers complain about the high risks of disclosing information their behaviors are easily influenced by low-level rewards. Therefore, consumer privacy calculus (Laufer & Wolfe 1977; Culnan & Bies 2003) is biased towards low benefits instead of high risks. It is assumed that consumers with higher risk attitudes/concerns will nonetheless disclose their personal information for lower-level of benefits in high-risk situations and vice versa (Smith et al. 2011).

Most privacy calculus and privacy paradox studies have limitations because of constructs like consumer willingness to disclose information (attitude) are not the actual disclosure behaviors (Xu et al. 2010) and intangible benefits of sharing personal data that are spread over a longer term in secondary exchange (Culnan & Bies 2003). Similar criticism from Smith et al. (2011) on privacy research is that such studies frequently captured user intentions, and not the actual behaviors, relying on theory of reasoned action assumptions that behaviors reflect user actual intentions (Fishbein & Ajzen 1975) which are measured at global rather than at situational level (Preibusch et al. 2013). This argument has been validated by disclosure behavior experimental studies in mobile and social networks. Keith et al. (2013) finds privacy paradox exists because individuals’ stated disclosure intentions do not reflect their actual disclosure behaviors. Sutanto et al. (2013) find users with privacy concerns were more than willing to share their information for personalization benefits on a trusted (privacy safe) mobile platform. Taddicken (2014) finds that social situations of ‘quid pro quo’ have a much higher impact than privacy concerns on willingness to disclose personal information in social networks. Another recent study has tried to address this issue by including observation on actual behavior induced by situational factors during a transaction or activity involving user information disclosure (Wilson & Valacich 2012). All these studies have exhibited a weak relationship between privacy concerns and willingness to disclose information even in actual disclosure situations.

There are few experimental studies that have tried to assign monetary values for personal information disclosures. Huberman et al. (2005) conducted a weight and age information disclosure auction with
127 students, who were asked to bid price values up to $100 on their disclosures. His participants were willing to accept money for their personal data despite privacy concerns. Similarly, Carrascal et al. (2011) were able to extract willing to accept money for personal information through an economic auction of 168 participants for identity, browsing and financial information through the Web giving away approximately €3000. Schreiner et al. (2012) have studied user behaviors through an experiment of 160 students in Germany by giving them an option of using free and premium services of social networking sites. The free service collects their personal information and displays advertisements, while the premium service charges a fee but does not collect their information. His participants were willing to pay €1.67 per month for privacy safe services. These studies have attempted to determine price valuations for personal information, only the Huberman & Carrascal study conducts a price auction in primary exchange (Boggozzi 1975; Culnan & Milberg 1998). But, their valuations were on select information disclosures.

Our study overcomes some of these limitations by observing actual consumer behaviors in a single utilitarian or primary exchange where personal information was disclosed for a payment. We believe primary exchanges where consumers are trading their personal information for a price is a better environment to capture consumer privacy valuation as it discloses a standardized economic value in terms of dollars (Preibusch et al. 2013). Results from first exchange auction experiments have proven to be better in finding valuation efficiently and these studies have found to be more generalizable (Jentzsch et al. 2012). Our privacy value measurement is a real monetary value obtained through an economic experiment in a realistic scenario. Therefore, our study should reveal a more accurate relationship between general privacy concerns (Westin-Harris 2003), individual information disclosure concerns (Smith et al. 1996; Malhotra et al. 2004; Dinev & Hart 2006), and disclosure behaviors (Xu et al. 2011; Keith et al. 2013). In sum, this study provides a more direct measure of consumers’ information disclosure behavior because of a primary exchange setting, where an individual is willing to accept a payment in exchange for disclosing her personal information. Our methodology is both unique and rigorous in examining the price valuation of personal data shared by consumers with different privacy segments, concerns, behaviors, and shed more light on the concept of privacy paradox.

3. RESEARCH STUDY

We shed more light on the privacy paradox with monetized valuation of personal information by consumers. We are exploring the relationship amongst three groups of variables --- consumers’ general privacy concerns (Westin 2000; Hann et al. 2007; Milberg et al. 2007), individual privacy concerns (Dinev & Hart 2006), and disclosure behaviors (Carlos 2005; Xu et al., 2011; Keith et al. 2013) and our dependent variable --- the price valuation of personal information obtained with an auction experiment. In our study, consumers were asked to provide their personal information in exchange for a payment. Prior research studies on privacy paradox have examined relationship between consumer privacy concerns and willingness to disclose (Smith et al. 1996; Malhotra et al. 2004; Dinev & Hart 2006) or in situational contexts like e-commerce (Chineppa & Sen 2007) or through personalization promise (Awad & Krishnan 2006) and mobile data sharing (Xu et al. 2010; Keith et al. 2013). We have found only two studies that have used experimental economic auction study on privacy valuation where consumers trade their online personal information for a monetary value (Huberman et al. 2005; Carrascal et al. 2011). Our study uses a generalized second-price auction mechanism and focuses on privacy valuation in a broader than the online context as in the prior valuation studies. Also, we surveyed the consumers on their privacy concerns and privacy behaviors in real-world situations and price valuation in willing to accept money for sharing personal information scenario. The research questions for this study are:

Q1. Do consumers’ general privacy concerns have an influence on their price valuation of personal information?
Q2. Do consumers’ individual disclosure concerns have an influence on their price valuation of personal information?
Q3. Do consumers’ disclosure behaviors in prior information sharing situations (Health providers, Internet, Mobile) have an influence on their price valuation of personal information?
Our research model, shown Figure 1, is explained below.

![Figure 1. Research Model](image)

### 3.1 Price Valuation of Personal Information (PVPI)

Prior studies have mentioned the importance of knowing the price valuation of personal information (PVPI). For example, Hui et al. (2007) point out that consumers were willing to disclose their personal information for monetary incentives. However, most studies have mainly observed price values through proxy constructs like willingness to accept or willingness to pay or through products price differences in privacy safe vs. privacy threatened environments. Beresford et al. (2010) and Jentzsch et al. (2012) have conducted laboratory and field experiments to determine price valuation of personal information, or what they refer to as monetizing privacy. In these studies, consumers were given choice of purchasing products from two competing online stores with one store requiring additional personal information in exchange for a lower price, and surveyed post experiment on their privacy beliefs and concerns. A large majority of consumers, both in the laboratory with over 500 participants in two studies and in one field experiment with 2300 participants opted for lower price store despite having to give their personal data while expressing privacy concerns (Jentzsch et al. 2012). Participants in the Hann et al. (2007) study were willing to share their information for secondary use on websites for about $30–$45. In the Schreiner et al. (2012) study participants were willing to pay between €1–1.67 per month for premium services of social networks like Facebook and Google. In several other studies, Internet users were sharing their personal information in exchange for personalization (Chellappa & Sin 2005) or other benefits like discounts (Spiekermann et al. 2001). Thus, most studies on monetizing privacy have used proxies of price valuation with no money. Huberman et al. (2005) and Carrascal et al. (2011) have used primary auction experiments with money. In the Huberman study users traded their age and weight information for an average price value of $57.56 and $74.06 respectively. The Carrascal study found a median price of €25 for user identity information, €7 for browsing history and social and €12-15 for financial interaction information. Both studies contexts have been limited to Web contexts and auctioned limited personal information.

Our dependent variable, PVPI, is prices offered by the participants for selling a variety of personal information from personal identity and demographic data to sensitive information like salary. This variable supports the view of privacy as an economic commodity (Laudon 1996; Smith et. al. 2011) where individuals view their personal information as an asset which can be exchanged for a tangible economic benefit. We would like to find out how consumers with varying privacy concerns behave in the auction environment and similarly, shed more light on the privacy paradox, namely, relationship between their information disclosure behaviors in their real-world privacy situations, like disclosing information at a physician’s office, Internet search engines, mobile phones and social networks. Therefore, our independent variables include those representing Westin privacy index segments,
stated privacy concerns and privacy disclosure behaviors. We also collected consumer demographics information but were not included in our model at this stage.

3.2 Independent Variables & Hypothesis

3.2.1 General Privacy Concerns (GPC)

The Westin-Harris privacy index studies that conducted over 30 studies between late 1970s and early 2000s with consumers measured general privacy concerns on information gathering and handling by firms (Kumaraguru & Cranor 2005). Their survey results aggregated over a long period of time provide consumer privacy concern differences through Westin Indexes. Individual privacy traits (Bansal et al. 2010) or personality differences (Smith et al. 2011) have found to affect privacy concerns. General privacy concerns have been used as proxy for privacy (Dinev et al. 2013) to probe consumers’ beliefs, attitudes and perceptions and has been studied as an independent variable by a large body of MIS research and measure its’ impact on actual disclosure behaviors like willingness to disclose information or participate in commercial transactions (Smith et al. 2011). Privacy concerns have also been used to measure consumer sentiment on privacy by opinion polls and research firms to determine individual feelings and attitudes on privacy (Harris & Westin, 1997) and to explore the impact of consumer fears on their sharing behavior (Schwartz & Edmondson, 1991). These are commonly used for categorizing users on their general privacy concerns (Lee et al. 2011). These studies found heterogeneity in terms of consumer general privacy concerns and categorized them into three segments, namely, fundamentalist, pragmatists and unconcerned (Harris, Louis & Assoc. and Westin 1991). In general,

- Privacy fundamentalists are very uncomfortable with current information practices and perceive them as a threat to their privacy and therefore cannot trust organizations when sharing their data,
- Privacy pragmatists are somewhat comfortable about the current information practices but perform a privacy calculus that weighs the risks of releasing personal information against the potential benefits (e.g. personalization or rewards).
- Privacy unconcerned are very comfortable with sharing data and have an opposite viewpoint of fundamentalist. They believe current information practices are not a threat to their privacy and are willing to share their personal information without much privacy concerns.

The Westin-Harris general privacy concern surveys and segmentation are a useful indicator of the consumer’s heterogeneity towards privacy concerns and risk beliefs as measured by the thousands of US consumers over a period of time, and their survey instrument has been validated by other privacy concern studies (Jensen et al. 2005). Our study uses the same three Westin-Harris consumer privacy survey questions to determine segments. Our subject segmentation was comparable to the Westin index segments. Namely, 25% of our subjects were fundamentalists compared to 27% in the Westin studies, 69% of our subjects were pragmatists compared to 60% in the Westin studies, and 6% of our subjects were unconcerned, which is smaller than 13% found in the Westin studies. Based on research from previous studies that found relationships between personal characteristics and privacy our hypothesis is that:

Hyp 1: General Privacy Concerns are related to their PVPI
   Hyp 1a. Consumers in fundamentalist segments will ask higher price for sharing their personal information
   Hyp 1b. Consumers in pragmatist segment will ask medium price for sharing their personal information
   Hyp 1c. Consumers in unconcerned segment will ask lowest price for sharing their personal information

3.2.2 Individual Disclosure Concerns (IDC)

Individual disclosure concerns are constructed from consumers’ personal experiences and risk perceptions from their information sharing commercial transactions (Smith et al. 2011). These concerns are different from general privacy concerns which are based on ability to control as a key factor due to government or society influence (Westin 1967) or from users’ cultural and environment
IDC also have considerable influence on their actual behaviors while sharing personal information as conceptualized by the privacy calculus research which suggest that individuals conduct a risk-benefit analysis when asked by organization to disclose their personal data (Culnan & Bies 2003). Individuals perceive risk factors based on their prior experiences and construct a perceived valuation of benefits (Xu et al. 2011). This perceived calculus valuation can be captured through survey instruments. Smith et al. (1996) has developed a higher level construct, concerns for information privacy which measures IDC through factors such as collection which focuses on how individual data is gathered by organizations, or secondary usage which captures individuals’ perception of data collected for one purpose and used for another, or user perceptions on errors protection against deliberate and accidental errors in individual data and accessibility of information held by others is readily available to others not authorized to access data. Malhotra, et al. 2004 have extended this instrument for Internet users’ privacy by adding two more factors. One is control – not having adequate control over their personal information held by others and other is awareness – awareness of information privacy practices by others (company, website or govt.).

The IDC factors in above instruments have been validated by several research studies (few examples include Culnan & Armstrong 1996; Dinev & Hart 2006; Xu et al. 2011) which have found a negative relationship between consumer privacy concerns and their willingness to disclose. Similarly, consumers perceive negatively towards personalization (Awad & Krishnan 2006). Prior research has also shown that individuals with high-levels of privacy concerns are very conservative in their responses to rewards such as personalization (Awad & Krishnan 2006). Other researchers have also included trust as complementary factor to privacy concerns and have found trust as having a positive influence on consumers in terms of their willing to disclose information (Belanger et al. 2002; Norberg et al. 2007). In our survey we have adapted a few questions from collection, secondary use, access and trust from prior studies to determine its’ impact on the price valuation of personal information. We wanted to limit the number of questions for our participants due to the overall time restrictions of our study. Based on prior research findings on the relationship between individual privacy concerns and willingness to disclose, we suggest following hypothesis to study the relationship between the consumers’ disclosure concerns and PVPI.

**Hyp 2:** Individual disclosure concerns are related to PVPI

**Hyp 2a.** Consumers with higher individual disclosure concerns will ask higher price for disclosing their personal information

**Hyp 2b.** Consumers with lower individual disclosure concerns will ask lower price for disclosing their personal information

### 3.2.3 Prior Disclosure Behaviors (PDB)

This variable captures consumers’ attitudes and concerns in terms of their prior behaviors in information sharing situations. Research on privacy has indicated the weakness of direct surveys and influence of cues on participants. Braunstein et al. (2011) has stated that direct surveys entice emotional responses on privacy concerns from users thereby biasing their responses towards higher risks. They conducted three different indirect surveys with users varying privacy warnings in each survey and found users privacy concerns increase as their privacy warning words escalated in the instructions. Their results indicate indirect survey questions are better indicators of privacy concerns. Similar support has been indicated by Leslie et al. (2010) through four experiments that users make irrational information disclosure decision when the context changes and signals of disclosure dangers are increased or lowered in different situations, and by Acquisti et al. (2009) who reports irrational behaviors by users willingness to pay valuations for privacy protection was opposite of their willingness to accept for disclosing data. Finally, Graeff & Harmon (2002) have used indirect data disclosing scenarios with their telephone survey to capture consumers’ awareness and concerns on loyalty cards for same reasons. Preibusch et al. (2013) meta-analysis study of survey and observational instruments also supports disclosure behaviors through scenarios over direct surveys as a better method to measuring privacy concerns.

Researchers have also used experimental scenarios to examine actual user information sharing behaviors in situational contexts due to biases of direct survey instruments. Participants are often
subject to choice behaviors that indirectly indicate their disclosure behaviors and privacy concerns (Preibusch et al. 2013). These experiments have generally supported the privacy paradox which states that consumers’ disclosure behaviors are opposite of their concerns, when enticed with rewards or incentives in a privacy exchange. Namely, consumers showing high-levels of general privacy or information disclosure concerns are still willing to disclose higher amounts of personal information in exchange for rewards (Acquisti and Grossklags 2005; Hann et al. 2007; Xu et al. 2011; Tsai et al. 2011; Jentzsch et al. 2012). Keith et al. (2013) in their study compare individual’s intent to disclose with actual information disclosures and found no support between privacy concerns and actual information disclosure but did a weak relationship between disclosure intentions and actual behavior suggesting disclosure behaviors are better predictors of actual behavior.

PDB will therefore be likely to have a stronger relationship with consumer price valuation of personal information. Consumers with less conservative disclosure behaviors are those who regularly give consent to their health-care providers for sharing their personal information, or share sensitive information, like salaries or grades, with friends and family members, or share their profiles, status and location information on search engines, social networks and mobile devices, respectively. In general, consumers with less conservative behaviors will be willing to sell their personal information at lower prices than those with more conservative behaviors.

Hyp 3: Prior Disclosure Behaviors are related to PVIP

Hyp 3a. Consumers with more conservative disclosure behaviors in prior information sharing situations will bid higher price for sharing their personal information

Hyp 3b. Consumers with less conservative disclosure behaviors in prior information sharing situations will bid lower price for sharing their personal information

4. METHODOLOGY AND RESULTS

4.1 Methodology

As described earlier, there is a lack of privacy research that uses a methodology to directly measure consumers’ valuation of their personal information. We propose using a methodology, based on the generalized second-price auction (GSP) mechanism (Edelman 2007; Varian 2007), to obtain consumers’ valuation of their personal information. Since this paper focuses on the privacy paradox issue rather than this methodology per se, we provide a concise description of the methodology in this section. A complete study of measuring consumers’ valuation of their personal information is presented in another paper of the authors.

The GSP mechanism is used by Google (AdWords) and some other search engines to determine the payment prices of advertisers when their advertising links get clicked. Advertisers submit bids for some keywords to a search engine, together with sponsored links related to the keywords. When a keyword matches a query of a search engine user, the search engine will show, along with the normal unpaid search result, a limited number of matching sponsored links. The order of listed sponsored links is based on the rankings of the bids for the keyword. If the user clicks on a link, the advertiser will pay to the search engine a fee corresponding to the advertiser’s bid for the keyword.

Although GSP is not an exactly truth-telling mechanism (Edelman 2007; Varian 2007), we have shown that, when the number of bidders (advertisers) is large, GSP approaches to a truth-telling mechanism. Therefore, in the context of privacy study, we can use the GSP mechanism to obtain consumers’ truthful valuation of their personal information. We have designed our study based on this idea.

To start the process, we sent a recruiting letter by mail and email to more than 10,000 potential participants, whose contact information were obtained from various sources, including the voter registration lists for several states in the United States, a consumer email list from a data aggregation company, and email lists from a university. We received about 500 responses expressing an interest in participating in the study. We then developed a website for the study and provided an access to the site for each respondent. An important message on the study website was that we were contacted by several marketing companies and data aggregators to help them to identify consumers who were
willing to sell their personal data to the companies for legitimate business use. This information is deceptive since we had not been contacted by any third party. This deceptive scenario, however, is necessary because the objective of the experiment is to obtain the participants’ valuation of their personal data that are truthfully reported under such a scenario. Because the deception was involved, the study plan was subject to a full review by the Institutional Review Board (IRB) and eventually received the IRB approval.

Given this scenario, 218 respondents participated in the study. During the process of the study (which was conducted online), they were required to complete a personal information form, which includes the participant’s full name and home address (which would be used to mail the payment check and thus were unlikely to be false). The other information includes email address, gender, date of birth, race, occupation, marital status, and income (for student, GPA and standard test scores instead). The participants then entered the bid prices as compensation for providing their personal information. The participants were provided with the total budget amount that the data collectors would spent for this study. We also ensured the participants that we would provide only their price information, not their personal data, to the data collectors. If a data collector agreed to purchase an individual’s data at the specified price, we would provide the individual’s email address to the data collector, who would then contact the individual directly for purchasing the data. In other words, whether and how much would an individual be paid depends on the price she specified. If the price was too high, she would not be paid but her personal information would not be released to the data collector either.

<table>
<thead>
<tr>
<th>Demographic Attributes</th>
<th>Category</th>
<th>Percentage (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gender</td>
<td>Female</td>
<td>51.8</td>
</tr>
<tr>
<td></td>
<td>Male</td>
<td>48.2</td>
</tr>
<tr>
<td>Age</td>
<td>18-23</td>
<td>27.9</td>
</tr>
<tr>
<td></td>
<td>24-29</td>
<td>27.4</td>
</tr>
<tr>
<td></td>
<td>30-39</td>
<td>18.6</td>
</tr>
<tr>
<td></td>
<td>40-49</td>
<td>13.7</td>
</tr>
<tr>
<td></td>
<td>50 and over</td>
<td>12.3</td>
</tr>
<tr>
<td>Race</td>
<td>African American</td>
<td>5.9</td>
</tr>
<tr>
<td></td>
<td>Asian</td>
<td>17.1</td>
</tr>
<tr>
<td></td>
<td>Hispanic</td>
<td>6.9</td>
</tr>
<tr>
<td></td>
<td>White</td>
<td>67.2</td>
</tr>
<tr>
<td></td>
<td>Other</td>
<td>2.9</td>
</tr>
</tbody>
</table>

Table 1. Demographic Statistics of Participants

The prices from the participants were then sorted in ascending order and the participants were paid accordingly up to the budget. In total, $4,000 were paid to 126 participants (this study is supported by a research grant from the National Institutes of Health). As part of this study, participants were asked to complete a survey, which includes those questions discussed earlier. A complete survey questionnaire is given in Table 3. Table 1 provides some demographic statistics of the participants. The participants’ occupations (which were not categorized) include managers, engineers, teachers, police officers, health professionals, human resource staff, IT professionals, as well as undergraduate and graduate students (which accounts for 36% of the participants). The mean bid price for the 218 participants is $372.44 (but only 126 of them who have lower bidding prices were actually paid).

4.2 Data Analysis

We first analyzed the prices by segmenting the study participants by the Westin-Harris privacy index. The first three questions in our survey were the same as Westin-Harris survey questions. This allowed us to use their formula to categorize our subjects into the three Westin segment. However, as mentioned earlier, the number of participants categorized as unconcerned is very small and not quite consistent with that in the Westin-Harris study. So, we combined the pragmatist and unconcerned into one group. The average prices by the two segments are shown in Table 2. The results show some support for our first hypothesis. In general, fundamentalist price bids are much higher than the other two segments.
We use regression analysis to study the relationships between the dependent variable PVPI and independent variables representing general privacy concerns, individual disclosure concerns and prior disclosure behaviors. Table 3 shows the list of independent variables used in the regression, along with related survey questions. These independent variables have been discussed in detail in Section 3.

<table>
<thead>
<tr>
<th>Category</th>
<th>Variable Name</th>
<th>Corresponding Survey Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Privacy Concerns</td>
<td>GPC1</td>
<td>1. Consumers have lost all control over how personal information is collected and used by companies. [5-point: 5 for ‘strongly agree’ … 1 for ‘strongly disagree’]</td>
</tr>
<tr>
<td></td>
<td>GPC2</td>
<td>2. Most businesses handle the personal information they collect about consumers in a proper and confidential way. [5-point]</td>
</tr>
<tr>
<td></td>
<td>GPC3</td>
<td>3. Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today. [5-point]</td>
</tr>
<tr>
<td>Individual Disclosure Concerns</td>
<td>IDC1</td>
<td>4. Sharing my data will help me access better products and services. [5-point]</td>
</tr>
<tr>
<td></td>
<td>IDC2</td>
<td>5. Sharing my data will make me more vulnerable to identity theft. [5-point]</td>
</tr>
<tr>
<td></td>
<td>IDC3</td>
<td>6. I am willing to share my data if I know and trust the data collector or website. [5-point]</td>
</tr>
<tr>
<td></td>
<td>IDC4</td>
<td>7. I am more concerned about privacy of my personal information given over the Internet compared with telephone, fax or mail. [5-point]</td>
</tr>
<tr>
<td>Prior Disclosure Behaviors</td>
<td>PDB1</td>
<td>8. How often do you sign the consent form to authorize the doctor and the affiliated medical institution to share your medical information with other doctors and institutions? [5-point: 5 for ‘never’ … 1 for ‘always’]</td>
</tr>
<tr>
<td></td>
<td>PDB2</td>
<td>9. How often do you share your salary information (or grade information for student) with your friends? [5-point]</td>
</tr>
<tr>
<td></td>
<td>PDB3</td>
<td>10. How frequently do you enter your full name in Google or other search engines? [5-point]</td>
</tr>
<tr>
<td></td>
<td>PDB5</td>
<td>12. I generally share location information on my mobile device with ___. [5-point: 5 ‘nobody’, 4 ‘GPS only’, 3 ‘do not use’, 2 ‘Wi-Fi &amp; cell tower’, 1 ‘all apps’]</td>
</tr>
<tr>
<td></td>
<td>PDB6</td>
<td>13. On Twitter, my privacy setting allows ___. [5-point: 5 ‘location detection’, 4 ‘others to find me’, 3 ‘do not use’, 2 ‘protected use’, 1 ‘public tweets’]</td>
</tr>
</tbody>
</table>

A square root transformation was taken for the price variable. Each of the variables was then plotted against the transformed price to confirm that the pair-wise relationship was linear. As a result, the basic regression model is:

\[
\sqrt{PRICE} = \alpha_1GPC1 + \alpha_2GPC2 + \alpha_3GPC3 + \beta_1IPC1 + \beta_2IPC2 + \beta_3IPC3 + \beta_4IPC4 + \gamma_1PDB1 + \gamma_2PDB2 + \gamma_3PDB3 + \gamma_4PDB4 + \gamma_5PDB5 + \gamma_6PDB6
\]

The results of the regression analysis based on this model are reported in Table 4. We also specify in the third column the expected direction of relationship between the independent variables and the dependent variable. A plus sign indicates that the relationship is expected to be positive while a minus sign indicates a negative relationship. The $R$-squared value of 0.1673 is relatively low and the coefficients of most of the independent variables are not statistically significant. In terms of the direction of the relationships, the signs of the coefficients for the three GPC coefficients are consistent with the expected signs. The signs of the coefficients for the four IDC variables are not very consistent with the expected signs (IDC2 and IDC3 are consistent while IDC1 and IDC4 are
The signs of the coefficients for the most of Privacy Disclosure Behaviors variables are consistent with the expected signs (PDB1 through PPDB4 are consistent while PDB5 and PDB6 are inconsistent).

Only three independent variables have statistically significantly relationships (at $\alpha = 0.1$) with the dependent variable with consistent direction. They are all Privacy Disclosure Behaviors variables (PDB1, PDB2 and PDB4).

<table>
<thead>
<tr>
<th>Independent Variables</th>
<th>Coefficients (p-value)</th>
<th>Expected Direction of Relationship with Dependent Variable</th>
</tr>
</thead>
<tbody>
<tr>
<td>GPC1</td>
<td>+0.7195 (0.3939)</td>
<td>+</td>
</tr>
<tr>
<td>GPC2</td>
<td>-0.9382 (0.2333)</td>
<td>-</td>
</tr>
<tr>
<td>GPC3</td>
<td>-0.4748 (0.5731)</td>
<td>-</td>
</tr>
<tr>
<td>IDC1</td>
<td>+0.0949 (0.8945)</td>
<td>-</td>
</tr>
<tr>
<td>IDC2</td>
<td>+1.0970 (0.2281)</td>
<td>+</td>
</tr>
<tr>
<td>IDC3</td>
<td>-0.5654 (0.4196)</td>
<td>-</td>
</tr>
<tr>
<td>IDC4</td>
<td>-0.8329 (0.1406)</td>
<td>+</td>
</tr>
<tr>
<td>PDB1</td>
<td>+0.9925 (0.0989)</td>
<td>+</td>
</tr>
<tr>
<td>PDB2</td>
<td>+1.3715 (0.0162)</td>
<td>+</td>
</tr>
<tr>
<td>PDB3</td>
<td>+0.2913 (0.6428)</td>
<td>+</td>
</tr>
<tr>
<td>PDB4</td>
<td>+1.4791 (0.0622)</td>
<td>+</td>
</tr>
<tr>
<td>PDB5</td>
<td>-0.5566 (0.3018)</td>
<td>+</td>
</tr>
<tr>
<td>PDB6</td>
<td>-1.4582 (0.0825)</td>
<td>+</td>
</tr>
</tbody>
</table>

$R^2 = 0.1672$

Table 4. Results of Regression Analysis

To further examine the relationship between the dependent variable and three groups of independent variables (General Privacy Concerns and Individual Disclosure Behaviors), we performed three statistical tests, based on the basic regression model, as specified below:

Test for GPCs: $H_0: \alpha_1 = \alpha_2 = \alpha_3 = 0$, $H_a$: At least one $\alpha_i$ is not zero.

Test for IDCs: $H_0: \beta_1 = \beta_2 = \beta_3 = \beta_4 = 0$, $H_a$: At least one $\beta_i$ is not zero.

Test for PDBs: $H_0: \gamma_1 = \gamma_2 = \gamma_3 = \gamma_4 = \gamma_5 = \gamma_6 = 0$, $H_a$: At least one $\gamma_i$ is not zero.

The $p$-value for the test for GPCs is 0.1876, suggesting that there is no statistically significant relationship between the dependent variable and any of the three GPC variables. The $p$-value for the test for IDCs is 0.3889, which also indicates that there is no statistically significant relationship between the dependent variable and any of the four IDC variables. The $p$-value for the test for PDBs is 0.0003, which suggests that there is a statistically significant relationship between the dependent variable and at least one of the six Privacy Disclosure Behaviors variables. This is expected because, based on the results shown in Table 3, we known that PDB1, PDB2 and PDB4 are statistically significant individually.

We believe the problem that some of the PDB variables are insignificant or even have an unexpected sign is due to the wording of the related questions. For example, the questions and answers for PDB5 (mobile device) and PDB6 (Twitter) are somewhat technical for the participants to understand, particularly if they did not have related experience.

5. DISCUSSION & CONCLUSIONS

This study focused on the understanding of privacy paradox in a first exchange where individuals can trade their personal information for a monetary value. Additionally, we used generalized second price
auction to extract price valuations from individuals which is considered more cost efficient (Preibusch et al. 2013) and proven to be more generalizable from laboratory to field (Jentzsch et al. 2012). Finally, we followed our auction study with a follow-up survey on participants’ privacy concerns and disclosure behaviors to determine the impact of individual differences on privacy attitudes and price calculus behaviors on their price valuations. A combined methodology of experiment and survey, though expensive and time consuming, promises a higher level of external validity (Priebusch et al. 2013).

Results from our study reveal interesting information on the privacy paradox. Field survey research has generally found that consumers’ actual disclosures do not match with their intended disclosures or individuals with high privacy concerns have been found to disclose personal and sensitive information in offline and online transactions (Smith et al. 2011; Belanger & Crossier 2011) with a general support that privacy concerns does not seem to affect individual’s willingness to disclose (Pavlov 2011). Similarly, situational experimental studies have found that intension to disclose does not map well to actual disclosures (Xu et al. 2010; Keith et al. 2013). Our regression model similarly indicates no support for general privacy concerns (GPC) or individual disclosure concerns (IDC). However, we found statistically significant relationships between some privacy disclosure behaviors (PDB) variables and price valuations of personal information (PVPI). This suggests prior disclosure behaviors are better predictors for privacy valuation. While GPC did not relate well to PVPI, we do find some support for Westin index segments on PVIP. Fundamentalists had much higher valuations than pragmatists and unconcerned.

There are several limitations both in our research methodology and data analysis. First, our sample size is limited and geographically restricted to the United States. While we sent out study invitation to thousands of people with over 500 responses agreeing to participate, only 218 actually participated due to sensitive nature of this study which required participants to reveal lot of personal information. Some participants in our auction experiment did not follow the rules of maximum price limits or following other instructions which may contaminate the results. More analysis on PVIP in a larger sample is necessary. With a larger sample size, we may be able to conduct other types of analysis on our survey data such as confirmatory factor analysis on higher level constructs like GPC, IDC and PDB and use SEM models for path coefficients to test our hypothesis.

While the results from our combined methodology on valuation of personal information are encouraging, more research with a more sophisticated data analysis, larger diversified sample, and rigorous methodology are needed to validate our findings. We plan to tap more participants in future from subject pools created for experimental research and use higher economic incentives to attract a bigger pool for our study. Future research also needs to examine relationships between all constructs of concerns for privacy (Smith et al. 1996; Malhotra et al. 2004; Dinev & Hart 2006) and PVPI to examine the cause of the privacy paradox. Similarly, a larger sample would allow us to look deeper into the consumer privacy calculus from the survey data and measure its impact on PVPI. For example, it would be interesting to find PVPI for consumers with higher risks and lower benefits attitudes and vice versa. Future research will also help us to understand the impact of trust on PVPI; for example, to examine whether individuals with higher trust in organization have lower economic values for their personal information.
References


Gage, D. 2013, 8:00 AM ET Wall street Journal Tech Customers More Attentive to Security in the Wake of NSA Leaks. December 12,


