Published in final edited form as:

Int J Bus Inf Syst. 2016 ; 23(3): 307–329. doi:10.1504/IJBIS.2016.10000351.

Unveiling consumer's privacy paradox behaviour in an economic exchange

Luvai F. Motiwalla and Xiao-Bai Li

Department of Operations and Information Systems, University of Massachusetts Lowell, Lowell, MA 01854, USA

Luvai F. Motiwalla: luvai_motiwalla@uml.edu; Xiao-Bai Li: xiaobai_li@uml.edu

Abstract

Privacy paradox is of great interest to IS researchers and firms gathering personal information. It has been studied from social, behavioural, and economic perspectives independently. However, prior research has not examined the degrees of influence these perspectives contribute to the privacy paradox problem. We combine both economic and behavioural perspectives in our study of the privacy paradox with a price valuation of personal information through an economic experiment combined with a behavioural study on privacy paradox. Our goal is to reveal more insights on the privacy paradox through economic valuation on personal information. Results indicate that general privacy concerns or individual disclosure concerns do not have a significant influence on the price valuation of personal information. Instead, prior disclosure behaviour in specific scenario, like with healthcare providers or social networks, is a better indicator of consumer price valuations.

Keywords

privacy paradox; privacy concerns; disclosure behaviours; privacy calculus; personal information; privacy valuation

1 Introduction

One side effect of the digital age is large amount of data creation and processing of personal data poses severe threats to individual privacy (Hansen, 2008). Information technology (IT) such as big data, data analytics and business intelligence have created enormous value for businesses, with this data, which now track and predict consumers' next move. This analytical knowledge is made available through network to interested and paying third parties leading to huge erosion of privacy, if not it's complete destruction. A *Wall Street Journal* report predicts that eventually privacy advocacy groups' objections will overwhelm corporate interests in data, and individuals will corrupted with free benefits from sharing personal information (Clark, 2014). This is a big shift from the 1990s when most (79%) US population in a Harris-Westin survey considered privacy as their fundamental right, written

in the US constitution, and majority (87%) had expressed concerns on their personal privacy (Westin, 2000).

In short, US public opinion on their personal information has gradually transitioned from a right 'to be left alone' (Westin, 1967) to a commodity that can be traded for economic or social value (Wang and Wu, 2014). Today, privacy is 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. Secondary data is nowadays traded among service providers like other commodities, priced on the quality of individual transactions, in the market place. Many online businesses have been collecting consumer information through second exchanges (Culnan and Bies, 2003) by providing consumers non-monetary benefits, either through personalisation incentives (Chellappa and Sin, 2005) or from loyalty programs (Krohn et al., 2002). Recent survey by Jenitzsch et al. (2012) found 47% of the service providers treated customer data as a commercial asset; and 48% revealed that they share data with third parties.

The recent data snooping incidents, like the National Security Agency (NSA) of the US collecting phone and other records on all Americans and foreign citizens has refocused consumer attention on privacy concerns and has intensified industry regulations, making data collection and sharing complex and expensive. Financial or healthcare services – which can use IT to become more personalised, efficient, and cost competitive – are contained due to information privacy concerns and regulations like HIPAA, FCRA, and others (Motiwalla and Li, 2013; Turhan and Vayvay, 2012). These regulations have created some confusion with no clear guidelines on consumer risks, inconsistent practices across media and platforms, different regulatory treatment across industries, like telecommunications and IT, and above all regulations that are not customer-driven (Clemons et al., 2014). This environment has created a need to understand consumer privacy behaviour in an economic setting, where personal information is treated like a commodity.

The IS research community has tried to understand information privacy concerns in an effort to improve online trade and commerce while protecting the consumer rights to privacy. Privacy concerns surface when consumers perceive information collection and sharing procedures of firms as an invasion of privacy (Smith et al., 1996). Individuals in western society often see privacy as a control and a rights issue. There are different ways to characterise information privacy. Westin (1967) defines privacy as the right of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is shared with others. Example violations of this right to be left alone are organisation collecting information without permission or consent through website cookies, spam advertising, pop-ups, and sponsored sites. These unwanted intrusions or interruptions are most prevalent concern amongst consumers (Clemons et al., 2014) and are the main focus of our study.

Overcoming privacy concerns is a popular issue in today's digital economy, because consumers are aware that organisations remotely and secretly collect significant amounts of their personal information and store it indefinitely (Adomavicius and Tuzhilin, 2005). Many

consumers meanwhile are unaware about the power of business intelligence and data analytics. They have been conditioned to accept privacy abuses and advertisements as cost of free internet services and personalisation does not cost consumers, it only allow companies to provide better service (Clemons et al., 2014). These myths and a general lack of awareness on privacy violations by consumers (Baek, 2014) have created a decision making phenomenon known as the *privacy paradox*, which basically states that consumers reporting high privacy concerns on surveys were nevertheless eagerly submitting their personal information for benefits in commercial transactions or other online or social situations (Smith et al., 2011). This suggests privacy concerns generally are not good predictors of consumer online behaviours (Norberg et al., 2007) and yet, they have significant influence on privacy policy and practices (Gandy, 2003), as well as determine economic value by way of consumer's willingness to disclose information (Dinev and Hart, 2006).

This lack of understanding on the privacy paradox has confused policy and practice on consumers' valuation on personal information. It also raises questions on how consumers value their personal information for money in economic exchanges and which privacy factors impact their valuations. Economic or utilitarian exchange is an environment where good and services are exchanged for immediate benefits either in form of money or other rewards (Bagozzi, 1975). Our research study investigates the relationship between consumers' privacy paradox behaviour and price valuation of personal information (PVPI) in a primary economic exchange setting. Namely, the actual disclosure behaviour of 218 consumers was observed through an economic experiment, where the participants were paid for sharing their personal information through an auction. This was followed by a post experiment survey on participants' privacy concerns which focused on three factors: general privacy concerns (GPC), individual disclosure concerns (IDC), and prior disclosure behaviours (PDB). Results indicate that GPC and IDC were not good indicators of consumers' PVPI. On the other hand, we find that consumer's PDB – such as sharing personal data with physicians, family members or friends or sharing personal information in social media (Facebook) – have a significant relationship on PVPI.

The rest of the paper is organised as follows. The next section reviews the relevant privacy literature and its limitation in understanding the PVPI within privacy paradox phenomenon. 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 GPC emerged in late 1960s (Westin, 1967). Westin's main focus was on individual privacy rights and control over information collected by organisations based on individuals' perceptions of distrust and fears of abuse with IT (Westin, 2000). The Harris-Westin consumer privacy surveys, from the late 1970s until 2004 have focused on several privacy domains from GPC to more focused areas in marketing, medical, and online commerce, and have resulted in a methodical privacy index that segments individuals into

three categories known as privacy fundamentalist, pragmatist and unconcerned (Kumaraguru and Cranor, 2005). The Westin privacy segmentation index 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. However, these surveys and their resulting segments do not provide information on how individual information disclosure decisions or behavioural intentions are affected by privacy concerns or how individuals' attest economic value on their personal data (Leslie et al., 2011).

This limitation has led to research that focuses on individual-level disclosures under risk uncertainty. With the large scale growth in the web and electronic commerce in the 1990s, privacy researchers were interested in consumer decision-making on remote data collection through web technologies like anonymous cookies for personalisation services (Culnan and Bies, 2003; Krohn et al., 2002) and sharing of their personal information with other firms (Li and Sarkar, 2013, 2014). From this research there emerged a consensus that consumers can experience both tangible and intangible benefits and risks, when disclosing their personal information (Culnan and Bies, 2003). Based on social exchange perspective, Laufer and Wolfe (1977) investigated IDC in situational contexts with high uncertainty of data sharing consequences and found that users' personal beliefs have big influence on their decision to disclose their personal information. This cost-benefit calculus was analysed through a second exchange which focuses on the intangible and long-term benefits of secondary uses of data and coined the term *privacy calculus* (Culnan and Bies, 2003).

Behavioural studies have used this privacy calculus model to analyse user privacy perceptions (Belanger and Crossler, 2011). The simplicity of this model has allowed researchers to group consumers' risk beliefs and privacy concerns into the cost factor and contrasts them with both tangible and intangible rewards into the benefits factor, and collectively understand its influence on consumers' willingness to disclose personal information (Smith et al., 2011). Risk measures include consumer attitudes towards data collection, storage protection, accuracy and control policies of the firms through concern for information privacy construct (Smith et al., 1996) 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. Benefit measures include personalisation, loyalty rewards or financial rewards (Acquisti, 2004).

The privacy calculus model addresses the limitation of Westin segmentations by providing additional details on individual decision making process under risk uncertainty of disclosing personal information and provides firms with measures to collect personal information with incentives (Li, 2012). Privacy calculus has been considered as a useful behavioural model (Laufer and Wolfe, 1977; Culnan and Bies, 2003; Dinev and Hart, 2006; Smith et al., 2011) or lens (Xu et al., 2010) to study consumer perceptions in second exchange. Privacy calculus analyses the trade-off between risks of disclosing personal information in relation to the benefits achieved from this information disclosure. Risk has been defined in this context of an individual's willingness to disclose information despite the negative consequences such as marketing messages, healthcare coverage loss, and others. Several studies that focus on

the calculus model have found that while consumers were highly concerned about privacy risks their actual information disclosure behaviours were often inconsistent with their stated privacy concerns (Norberg et al., 2007). This has led to a number of follow-up studies on *privacy paradox*.

Privacy paradox research finds consumers' actions (actual behaviours) contradict with their stated privacy concerns when disclosing personal information in exchange for rewards (Leslie et al., 2011; Jensen et al., 2005; Norberg et al., 2007; Keith et al., 2013). While consumers complain about the high risks of disclosing information their behaviours are easily influenced by low-level rewards. Consumer privacy calculus is biased towards low benefits instead of high risks. Privacy paradox reveals that consumers with higher stated risk attitudes or concerns may nonetheless disclose their personal information for lower-level of benefits and vice versa.

Most privacy calculus and privacy paradox studies have limitations because of constructs like *consumer willingness to disclose information* (attitude) are not the actual disclosure behaviours (Xu et al., 2010) and are in form of perceptual benefits that consumers expect over time in a second exchange (Culnan and Bies, 2003). Similar criticism from Smith et al. (2011) on privacy research is that such studies frequently captured user intentions, but not the actual behaviours. Often, consumer willingness to disclose information is measured at global rather than at situational level (Preibusch, 2013). Privacy paradox has been found in several experimental studies on information disclosure behaviour in mobile and social networks. Keith et al. (2013) found it existed in mobile environments because individuals' stated disclosure intentions do not reflect their actual disclosure behaviours. Similarly, Sutanto et al. (2013) found that users with privacy concerns were more than willing to share their information for personalisation benefits on a trusted (privacy safe) mobile platform. Likewise, Taddicken (2014) found privacy paradox existed in social networks as users were willing to disclose personal information on a '*quid pro quo*' basis with other users, rather than influenced by privacy concerns. All these studies have exhibited a weak or no relationship between privacy concerns and willingness to disclose information in actual disclosure situations.

There are few economic experimental studies that have tried to understand monetary valuation of personal information. Huberman et al. (2005) conducted a weight and age information disclosure auction with 127 students, who were willing to accept money for their personal data despite privacy concerns. Carrascal et al. (2013) found users willing to accept money in exchange for personal information, as well as browsing and shopping information in an economic auction with 168 participants. Schreiner and Thomas (2013) observed user behaviours of 160 students in Germany by giving them an option of using free and premium services of social networking sites. The free service collected their personal information and displayed advertisements, while the premium service charged a fee, but does not collect their information. Most users were willing to pay only about €1.50 per month for the premium service. These studies have attempted to determine price valuations for personal information, with a few studies in economic exchange (Huberman et al., 2005; Carrascal et al., 2013). However, these studies do not examine the privacy paradox problem.

Thus, existing research on information privacy states that most consumers conduct risks and benefits privacy calculus before disclosing their personal information (Smith et al., 1996; Culnan and Bies, 2003; Dinev and Hart, 2006). Risk factors include concerns on data collection methods, secondary usage, error, access, control and awareness (Hong and Thong, 2013; Chinaei et al., 2012; Jamal et al., 2013). Benefit factors typically include personalisation, financial rewards and social adjustments (Smith et al., 2011; Almadhoun and Dominic, 2014). We contribute to this body of research by measuring PVPI in a primary economic exchange. Previous studies on privacy paradox have examined privacy calculus behaviour in secondary exchanges (Culnan and Bies, 2003) where consumers trade their personal information for future non-monetary benefits such as social values. The dependent variable in these studies are either consumers' willingness to disclose (Dinev and Hart, 2006), willingness to pay (Schreiner and Thomas, 2013), or willingness to share for personalisation (Awad and Krishnan, 2006). These are all proxy for PVPI.

Our study overcomes this limitation by observing privacy paradox in a primary economic exchange where consumers' actual disclosure behaviour is captured through an auction experiment. Our dependent variable was actual PVPI as subjects in our study were required to disclosed their personal information for a monetary value. In a comprehensive review of research instruments used in privacy studies, Preibusch (2013) concludes that economic exchanges are a better method for capturing consumer price valuations as they allow a discloser of a standardised economic value in terms of a currency. Results from economic experimental studies have proven to be better in truthful valuations efficiently and results found to be more generalisable (Jenitzsch et al., 2012; Carrascal et al., 2013). Therefore, our approach should reveal a more accurate privacy calculus behaviour. Economic experiments generally do a better job in revealing consumers' true preferences about privacy concerns and promise better level of external validity (Preibusch, 2013), and therefore do a better job in unveiling the privacy paradox. Furthermore, bid prices obtained from the auctions are price points specified by users providing a continuum of cardinal values instead of the frequency counts obtained by an ordinal scale of a survey (Preibusch, 2013). The auction data should enable us to perform better statistical analysis of the relationship between our dependent variable of price valuation and our independent variables of various privacy concerns.

3 Research study\

Our research model, shown in Figure 1, attempts to unveil the consumer privacy paradox behaviour with monetised PVPI. It explores the relationship between our independent variables – consumers' GPC (Westin, 2000; Hann et al., 2007), IDC (Dinev and Hart, 2006), and PDB (Xu et al., 2011; Keith et al., 2013) and our dependent variable – PVPI (Huberman et al., 2005; Carrascal et al., 2013) 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 and Hart, 2006) or in situational contexts like e-commerce (Chellappa and Sen, 2005) or through personalisation promise (Awad and Krishnan, 2006) and mobile data sharing (Xu et al., 2010; Keith et al., 2013). We have found very few studies that used experimental

economic auctions on price valuation where consumers trade their online personal information for a monetary value (Huberman et al., 2005; Carrascal et al., 2013). None of them addresses the privacy paradox issue.

The research questions for our study attempts to probe the consumers' privacy calculus behaviour with independent variables focusing on costs or risk measures such as privacy concerns, disclosure concerns and disclosure behaviours in prior real-world situations and dependent variable focusing on benefit in terms of their PVPI. The study was in form of an economic experiment in a primary exchange auction. Our research study is designed to provide answers to following questions:

Q1 Do consumers' GPC have an influence on their PVPI?

Q2 Do consumers' IDC have an influence on their PVPI?

Q3 Do consumers' disclosure behaviours in prior information sharing situations have an influence on their PVPI?

3.1 Price valuation of personal information

Prior studies have mentioned the importance of knowing the PVPI. For example, Hann 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 threaten environments. Jenitzsch et al. (2012) have conducted laboratory and field experiments to determine PVPI, or what they refer to as *monetising 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 2,300 participants opted for lower price store despite having to give their personal data (Jenitzsch 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 and Thomas (2013) 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 personalisation (Chellappa and Sin, 2005) or other benefits like loyalty rewards (Krohn et al. 2002). Thus, most studies on monetising privacy have used proxies of price valuation with no money change hands. Huberman et al. (2005) and Carrascal et al. (2011) have used auction experiments with monetary payments. 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 media information and €12–15 for financial interaction information. Both studies' contexts have been limited to web and auctioned limited personal information with single winner per auction.

Our dependent variable, PVPI, is the price bids offered by the participants for selling their personal information from personal identity demographic data and other information. This

variable supports the view of privacy as an economic commodity where individuals view their personal information as an asset which can be exchanged for a tangible economic benefit. In this study we were interested in how consumers with varying privacy concerns behave in an economic exchange through an auction experiment.

3.2 General privacy concerns

Alan Westin, with Harris Associates consulting firm, has conducted over 30 studies between late 1970s and early 2000s measuring GPC on information gathering and handling by firms (Kumaraguru and Cranor, 2005). Their survey results aggregated over a long period of time measure consumers' GPC and use the results to create Westin privacy segments. GPC have been used as proxy for privacy (Smith et al., 2011) to probe consumers' risk beliefs, attitudes and perceptions and have been studied as independent variables by a large body of IS research with dependent variable like willingness to disclose information (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 (Westin, 2000) and to explore the impact of consumer fears on their sharing behaviour. These studies found heterogeneity in terms of consumer GPC and categorised them into three segments, namely, *fundamentalist*, *pragmatists* and *unconcerned* (Westin, 2000). In general,

- Privacy *fundamentalists* are very uncomfortable with current information practices and perceive them as a threat to their privacy and therefore cannot trust organisations with their data; therefore, they are generally unwilling to disclose their personal information.
- 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. personalisation or rewards); therefore, they are reluctant in disclosing their personal information.
- 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; therefore are generally willing to share their personal information.

The Westin GPC 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 used the same GPC survey questions to determine three Westin segments. Our participant segmentation was comparable to the Westin segments. Namely, 25% of our participants were fundamentalists compared to 27% in the Westin studies, 69% of our participants were pragmatists compared to 60% in the Westin studies, and 6% of our participants were unconcerned, which is much smaller than 13% found in the Westin studies. Therefore, we combine the last two segments into one segment. Our hypothesis is based on research from prior studies that similarly found relationship between consumers' privacy concerns and willingness to disclose:

Hyp 1 GPC are related to PVPI.

Hyp 1a Consumers in fundamentalist segments will ask higher price for sharing their personal information.

Hyp 1b Consumers in pragmatist and unconcerned segments will ask medium to lower price for sharing their personal information.

3.3 Individual disclosure concerns

IDC are constructed from consumers' personal experiences and risk perceptions from their information sharing commercial transactions (Smith et al., 2011). These concerns are different from GPC 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 (Laufer and Wolfe, 1977). IDC also have considerable influence on their actual behaviours while sharing personal information as conceptualised by the privacy calculus research which suggest that individuals conduct a risk-benefit analysis when asked by organisation to disclose their personal data (Culnan and 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 factors such as *collection* which focuses on how individual data is gathered by organisations, *secondary usage* which captures individuals' perception of data collected for one purpose and used for another, *error protection* focusing on deliberate and accidental prevention of errors with individual data stored in firms, and *accessibility* which focuses on information availability to unauthorised third parties. Malhotra et al. (2004) have extended this instrument for internet users' privacy by adding two more factors: *control* – not having adequate control over their personal information held by others; and *awareness* – awareness of information privacy practices by others (company, website or government).

The IDC factors in above instruments have been validated by several studies (Dinev and Hart, 2006; Xu et al., 2010, 2011) which have found a negative relationship between IDC and willingness to disclose personal information. Similarly, research has also demonstrated that individuals with high-levels of disclosure concerns are very conservative in their responses to benefits such as personalisation (Awad and Krishnan, 2006). In our survey, we have adapted questions from collection, secondary use and access factors used in prior studies to determine its' impact on the PVPI. While prior studies have studied the relationship between IDC and willingness to disclose, our focus is on the relationship between IDC and PVPI. Therefore, we propose that

Hyp 2 IDC are related to PVPI.

Hyp 2a Consumers with higher IDC will ask higher price for sharing their personal information.

Hyp 2b Consumers with lower IDC will ask lower price for sharing their personal information.

3.4 Prior disclosure behaviours

This variable captures consumers' attitudes and concerns in terms of their prior behaviours 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 Lewis et al. (2008) 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 (2004) who reports irrational behaviours by users willingness to pay valuations for privacy protection was opposite of their willingness to accept for disclosing data. Graeff and Harmon (2002) have used indirect data disclosing scenarios with their telephone survey to capture consumers' awareness and concerns on loyalty cards for same reasons. A meta-analysis study of survey and observational instruments by Preibusch (2013) also supports disclosure behaviours through scenarios over direct surveys as a better method for measuring privacy concerns.

Researchers have also used experimental scenarios to examine actual user information sharing behaviours in situational contexts due to biases of direct survey instruments. Participants are often subject to choice behaviours that indirectly indicate their disclosure behaviours and privacy concerns (Preibusch, 2013). These experiments have generally demonstrated the privacy paradox which states that consumers' disclosure behaviours are inconsistent with their concerns when enticed with rewards or incentives. Consumers showing high-levels of information disclosure concerns are still willing to share large amounts of personal information in exchange for rewards (Leslie et al., 2011; Hann et al., 2007; Xu et al., 2011; Tsai et al., 2011; Jenitzsch et al., 2012). Keith et al. (2013) compare individual's intent to disclose with actual information disclosures and found a weak relationship between disclosure intentions and actual behaviour, suggesting that PDB may be better predictors of actual behaviour and that specific risk situations overwhelm consumers' GPC.

Hence, PDB is likely to have a stronger relation with PVIP. Consumers with less conservative disclosure behaviours are those who regularly give consent to their healthcare providers for sharing their personal information, share private 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 behaviours will be willing to sell their personal information at lower prices than those with more conservative behaviours. Therefore, we propose that

Hyp 3 PDB are related to PVPI.

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

Hyp 3b Consumers with less conservative disclosure behaviours in prior information sharing situations will ask 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 in an economic exchange

setting. Economic exchange environment is better for truthful valuation as prior studies have reported that a large percent of consumers hide or provide fake information to protect their privacy in online settings (Wang and Wu, 2014). Specifically, in the context of privacy study, we can use the auction mechanism to obtain consumers' truthful valuation of their personal information. We have designed our study based on this idea.

Our study uses an experimental auction mechanism to obtain consumers' true valuation of their personal information. We provide a concise description of the methodology in this section because the focus of this paper is on understanding consumers' privacy paradox behaviour, rather than on the experimental auction methodology per se.

Our auction pricing mechanism is similar to those used by Google (AdWords) and some other search engines to determine the payment prices of advertisers when their advertising links get clicked (Edelman et al., 2007; Varian, 2007). 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. In our experiment, the participants engage in an auction to sell their information rather than to buy. The winners are selected by their bid price from the lowest to the highest, up to a budget limit. A participant will most likely bid based on her true valuation of her personal information – if she bids below her true valuation and wins, she will regret for selling her information too cheap; if she bids above her true valuation, she will likely not be paid.

To start the process, we sent a recruiting letter by mail and e-mail 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 USA, a consumer e-mail list from a data aggregation company, and e-mail 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 was deceptive since we had not been contacted by any third party. This deceptive scenario, however, was necessary because the objective of the experiment was 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 experimental auction 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 e-mail address, gender, date of birth, race, occupation, marital

status, and income. 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 spend for this study. We also ensured the participants that we would share 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 e-mail 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.

The prices from the participants were then sorted in ascending order and the participants were paid accordingly up to the budget. 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 4. We purposely limited the number of questions due to the overall time restrictions of our study which included the auction experiment. Table 1 provides some demographic statistics of the participants. The participants' occupations (which were not categorised) 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).

4.2 Data analysis

We first analysed the prices by the Westin privacy segments. The first three questions in our survey were the same as Westin-Harris survey questions. This allowed us to use their formula to categorise our participants into the three Westin segments. However, as mentioned earlier, the number of participants categorised as unconcerned was very small and not proportionate with that in the Westin studies. So, we combined the pragmatist and unconcerned into one group. The average prices both combined and by the two segments are shown in Table 2. The mean bid price for the 218 participants is \$372.44 (calculated based on the prices specified by all participants, including those who were not paid). The results show some support for our first hypothesis. In general, mean bid price of the fundamentalist were much higher than the mean bid price of the pragmatist and unconcerned, suggesting that privacy concerns may have led the fundamentalist to ask for higher price than the pragmatist or unconcerned participants.

To confirm whether these mean bid price differences were significant, we analysed differences between the two means through a paired t-test. The results shown in Table 3 ($p = 0.001$ in equal variances assumed or not assumed) suggest that there is a statistically significant difference between the price bids of the two groups (fundamentalist vs non-fundamentalist).

Table 4 shows the list of independent variables representing GPC, IDC, and PDB used in our study, along with related survey questions and answers that used a traditional five-point Likert scale for GPC and IDC items and custom five-point scale for PDB items. These variables were discussed in detail in the previous section.

Table 5 shows the mean, standard deviation and frequency distribution of our sample on the survey questions. On the GPC questions, majority of our participants do not like how data is collected, used and handled properly by firms, and disagree with existing laws and practices to protect their personal information. In terms of IDC, participants from our study were willing to share their data if they knew and trust the firm collecting their information but they also feel that sharing their personal information (PI) could make them more vulnerable to identity crimes and were generally more concerned sharing information over the internet compared with traditional communication media. Finally, results were somewhat mixed in the PDB area. While they were comfortable sharing their health data with medical providers, they were not eager on sharing information on social networks, entering personal information on search engines, or sharing their location information on mobile devices. This suggests that participants' privacy concerns and disclosure behaviours were similar to results from prior studies in terms of GPC and participants are concerned about disclosing their personal information unless they trust or know the other party, or when information sharing is clearly beneficial (like for medical reasons).

Next, we use regression analysis to study the relationships between the dependent variable, PVPI, and the independent variables. Originally, the relationships between the price variable and independent variables are nonlinear. Therefore, a square root transformation was taken for the price variable (*SqrtPrice*). Each of the independent variables was then plotted against the transformed price variable to confirm that the pair-wise relationship was linear. The basic regression model used in our study is:

$$\begin{aligned} SqrtPrice = & \alpha_1 GPC1 + \alpha_2 GPC2 + \alpha_3 GPC3 \\ & + \beta_1 IPC1 + \beta_2 IPC2 + \beta_3 IPC3 + \beta_4 IPC4 \\ & + \gamma_1 PDB1 + \gamma_2 PDB2 + \gamma_3 PDB3 + \gamma_4 PDB4 + \gamma_5 PDB5 + \gamma_6 PDB6 \end{aligned}$$

The results of the regression analysis based on this model are reported in Table 6. We also specify in the third column the expected direction of relationship between each independent variable 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 0.1672 is relatively low and the coefficients of most of the independent variables are not statistically significant. This indicates that most of the independent variables do not explain well about the price value of personal information.

In terms of the direction of the relationships, the signs of the coefficients for the three GPC coefficients are consistent with the expected signs. This suggests that GPC have some influence on consumer price valuations. For example, participants in our study who were negative about how personal information is handled by firms generally had higher price valuation than participants with positive or neutral attitudes towards firms' handling of data. This also suggests that firms with better reputation, image and privacy policies could obtain personal information at a lower price or would face lower resistance from their consumers in sharing personal information. However, large *p*-values associated with the GPC variables suggest that GPC variables were not significantly related to price valuations.

The signs of the coefficients for the four IDC variables are mixed: while IDC2 and IDC3 are consistent with the expected signs, IDC1 and IDC4 are inconsistent. Furthermore, large p -values associated with IDC2 and IDC3 suggest that their effects were not statistically significant even though their signs are consistent with expectations. In general, therefore, we do not observe a significant relationship between any of the IDC variables and the price valuation. In particular, the IDC1 and IDC4's inconsistent signs confirms the privacy paradox found in earlier studies, namely consumers tend to behave differently from their stated privacy concerns when actually disclosing their personal information.

The signs of the coefficients for the most of PDB variables are consistent with the expected signs (PDB1 through PDB4 are consistent while PDB5 and PDB6 are inconsistent). Participants who normally consent on sharing their health data with other health organisations (PDB1), or share personal information like salary or grades with friends and family (PDB2), or are less concerned about exposing their identities to search engines or website (PDB3), or disclose their information on social networks like Facebook (PDB4), were generally asking lower prices in exchange for their personal information than their counterparts. The results of PDB5 (about sharing location information on mobile devices) and PDB6 (about privacy settings on Twitter) are inconsistent with the expected results. We believe this is mainly because participants might not have clearly understood survey questions on those two items due to their lack of experience in using the features mentioned in the questions. A high percentage (58.7%) of our participants were not Twitter users and unaware of Twitter's privacy settings.

To further examine the relationship between the dependent variable and three groups of independent variables (GPC, IDC and PDB), we performed the following three partial F tests (Kutner et al., 2005), based on the basic regression model:

- test for GPCs: $H_0: \alpha_1 = \alpha_2 = \alpha_3 = 0$, H_a : at least one α_i is not zero
- test for IDCs: $H_0: \beta_1 = \beta_2 = \beta_3 = \beta_4 = 0$, H_a : at least one β_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 γ_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 price valuation 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 price valuation 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 price valuation and at least one of the six PDB variables. In fact, it is clear from Table 6 that three independent variables (i.e., PDB1, PDB2 and PDB4) have statistically significantly relationships (at $\alpha = 0.1$) with the price valuation and with a consistent direction. They are all privacy disclosure behaviours (PDB) variables.

Based on our analysis of the results, we find that GPC and IDC do not have a significant relationship with the PVPI. The results from some of the IDC variables actually demonstrate the privacy paradox phenomenon. On the other hand, PDB in specific scenarios are more consistent with consumers' price valuations. This suggests that a better approach for

understanding privacy concerns of consumers is by observing their actual behaviour in real data sharing contexts as previously suggested by extant privacy paradox research. Context-specific behaviour is much better predictor of privacy behaviours than stated privacy concerns.

5 Discussion and conclusions

While our study is not a full-fledge field experiment, by combining economic experiment with field survey, we provide a more rigorous method to study the privacy paradox. The key unique contributions from this study are:

- Our focus on the understanding of privacy paradox in an economic exchange where consumers can trade their personal information for a monetary value. To our knowledge, there has not been a study of this kind in the literature. Economic exchanges are generally more effective than second exchanges because consumers get immediate gratification from monetary benefits in exchange for revealing their true valuations for privacy (Preibusch, 2013).
- Our use of an economic experiment with a deceptive scenario to extract price valuations from individuals in an auction, which is considered more cost efficient (Preibusch, 2013) and proven to be more generalisable from laboratory to field (Jenitzsch et al., 2012) and a good way to accurately capture consumer's true disclosures under risk (Keith et al., 2013).
- Our focus on measuring privacy benefits through actual disclosure of personal information in exchange for a monetary payment, instead of using proxy variables to measure privacy construct that were used in prior studies (Smith et al., 2011) like willingness to disclose information.
- Combining an economic experimental study with a survey on participants' privacy concerns and disclosure behaviours to determine the impact of privacy calculus behaviours on their actual price valuations of personal information.
- Not limiting our sample to student population; our sample includes both students (36% of our sample) and non-students (64%) with diversified age groups, educational, occupational and ethnic backgrounds coming from a large geographical area (22 different US states).
- Categorising our sample by using Westin-Harris survey instrument thereby leveraging Westin segments to demonstrate the different price valuations by each category. Despite their shortcomings, Westin privacy instrument and segmenting continues to be used widely (Preibusch, 2013).

The results from our study reveal interesting insights on the privacy paradox. Field survey research has often found that consumers' privacy and disclosures concerns do not match with their intended disclosure behaviour in field setting. That is, individuals with high privacy concerns have been found to readily disclose personal and sensitive information in

field setting (Smith et al., 2011; Belanger and Crossier, 2011) or basically, privacy concerns do not seem to affect individual's willingness to disclose. Similarly, situational experimental studies have found that willingness to disclose does not map well to actual disclosures (Xu et al., 2010; Keith et al., 2013). Our data analysis similarly indicates only directional support for GPC and no support for IDC. However, we found statistically significant relationships between some PDB variables and PVPI. This suggests that PDB in situational contexts are better predictors for price valuation and a better measure of privacy. We also found some support for Westin segments. Fundamentalists had much higher price valuations than pragmatists and unconcerned.

This study has significant theoretical and practical implications. Our results do not completely support the predictions by some privacy experts (Clemons et al., 2014; Clark, 2014) that corporate interest on data collection and analysis will erode privacy and corrupt consumers to share their personal information. We do not find majority support for this claim although we do see some commoditisation of privacy through sharing of personal information. Therefore, data aggregators and marketers need to approach data collection with caution and tailor their message depending on consumer privacy segment. For example, privacy fundamentalists will not be easily influenced by the privacy economy; they are not interested in nor comfortable with sharing their information for economic benefit. Fundamentalist would require much higher price value and convincing to share their information. Fundamentalist behaviour was also evident indirectly from our data collection process where more than half of the 500 respondents who had initially agreed to participate in our study did not respond after they saw they had to reveal their personal information in order to be paid. Thus, pricing strategies must take into account consumer privacy calculus for attracting consumers into sharing their personal information.

Our study has limitations both in our research methodology and data analysis. First, our sample size was limited and geographically restricted to the North America. Also, our sample could be biased due to self-selection process where participants with higher privacy concerns or fundamentalists may have opted to not participate. We had sent out study invitation to thousands of people, out of which 500 responses agreeing to participate and only 218 actually participated with their personal data and price bids. Also, due to small size of unconcerned participants we could not separate the two groups (pragmatist and unconcerned) of participants. Second, because our experiment was conducted online we could not control participants' behaviours for consistency. Also, our post-experiment survey did not measure all the items of concern for information privacy (Smith et al., 1996) or internet user concerns for privacy constructs (Malhotra et al., 2004) due to time constraints of our study. But, unlike previous studies, we capture consumers' real price disclosures instead of their willingness to disclose. Finally, current study did not focus on consumers' situational privacy contexts under which they are sharing this information. Our situational context was broad where they were told to share data for marketing firms. In future, we plan to focus on PDB and provide more specific situational scenarios for sharing information to better observe the privacy calculus behaviour and privacy paradox effect on their price valuation. Also, a larger and global sample will allow us to conduct more sophisticated statistical analysis on our survey data such as confirmatory factor analysis on higher level

constructs like GPC, IDC and PDB and use structured equation 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 further validate our findings. We plan to tap more participants in future from participant pools created for experimental research or through crowdsourcing to attract a bigger pool for our study. Future research also needs to examine relationships between privacy concerns constructs from prior studies (Smith et al., 1996; Malhotra et al., 2004; Dinev and Hart, 2006) and price valuations to examine the underlying causes of the privacy paradox. Similarly, a larger sample would allow us to get deeper understanding of the privacy calculus theory (Li, 2012) from the survey data and measure its impact on price valuations. For example, it would be interesting to find price valuations for consumers with higher risks and lower benefits attitudes and vice versa through economic exchanges. A larger sample would also help us to understand the impact of trust on price valuations; for example, to examine whether individuals with higher trust in organisation have lower price values for their personal information.

Acknowledgments

This research was supported in part by the National Library of Medicine of the National Institutes of Health (NIH) under Grant Number R01LM010942. The content is solely the responsibility of the authors and does not necessarily represent the official views of NIH.

Biographies

Luvai F. Motiwalla is a Professor of Management Information System (MIS) and the Chair of the Operations and Management Information Systems Department at the University of Massachusetts Lowell. He earned his MS and PhD degrees in MIS, in 1989, from the University of Arizona. His current research mainly focuses on mobile banking, enterprise systems and information privacy. His teaching areas include e-business, enterprise systems and MIS. He has published a book on ERP, several articles in refereed journals like *JMIS*, *Info&Mgmt* and *CACM*. He also has research grants from the NIH, NSF, US DoE, PeopleSoft, Davis Foundation, CT-Dept. of Health Services, IBM, NCR and US Army.

Xiao-Bai Li is a Professor of MIS in the Department of Operations and Information Systems at the University of Massachusetts Lowell. He received his PhD in Management Science from the University of South Carolina in 1999. His research focuses on data mining, data privacy and information economics. He has received funding for his research from the National Institutes of Health (NIH) and National Science Foundation (NSF). His work has appeared in *Information Systems Research*, *Management Science*, *MIS Quarterly*, *Operations Research*, *IEEE Transactions (TKDE, TSMC, TAC)*, *Communications of the ACM*, *Decision Support Systems*, *INFORMS Journal on Computing*, among others.

References

- Acquisti, A. Proceedings of the 5th ACM Conference on Electronic Commerce. ACM Press; New York: 2004. Privacy in electronic commerce and the economics of immediate gratification; p. 21-29.

- Adomavicius G, Tuzhilin A. Personalization technologies: a process-oriented perspective. *Communications of the ACM*. 2005; 48(10):83–90.
- Almadhoun NM, Dominic PDD. Investigation of perceived security, privacy and trust on social networking sites for stakeholder relationships development in Malaysian universities. *International Journal of Business Information Systems*. 2014; 15(1):1–21.
- Awad N, Krishnan M. The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly*. 2006; 30(1):13–28.
- Baek YM. Solving the privacy paradox: a counter-argument experimental approach. *Computers and Human Behavior*. 2014 Jun.38:33–42.
- Bagozzi RP. Marketing as exchange. *Journal of Marketing*. 1975; 39(4):32–39.
- Belanger F, Crossler RE. Privacy in the digital age: a review of information privacy research in information systems. *MIS Quarterly*. 2011; 35(4):1017–1041.
- Braunstein, A.; Granka, L.; Staddon, J. Indirect content privacy surveys: measuring privacy without asking about it. *Proceedings of the 7th Symposium on Usable Privacy and Security*; New York: ACM Press; 2011. p. Article 15
- Carrascal, JP.; Riederer, C.; Erramilli, V.; Cherubini, M.; de Oliveira, R. Your browsing behavior for a Big Mac: economics of personal information online. *Proceedings of the 22nd International Conference on World Wide Web*; New York: ACM Press; 2013. p. 189-200.
- Chellappa RK, Sin RG. Personalization versus privacy: an empirical examination of the online consumer's dilemma. *Information Technology and Management*. 2005; 6(2):181–202.
- Chinaei AH, Adl RK, Liang C, Barker K. Decentralised privacy preservation in social networks. *International Journal of Business Information Systems*. 2012; 9(4):402–414.
- Clark, R. *Wall Street Journal: Leadership Reports*. 2014 Jul 7. Future of privacy: only the rich will have it.
- Clemons, E.; Wilson, J.; Fujie, J. Investigations into consumers preferences concerning privacy: an initial step towards the development of modern and consistent privacy protections around the globe. *Proceedings of the 47th Hawaii International Conference on System Science*; Washington, DC: IEEE Computer Society; 2014. p. 4083-4092.
- Culnan MJ, Bies RJ. Consumer privacy: balancing economic and justice considerations. *Journal of Social Issues*. 2003; 59(2):104–115.
- Dinev T, Hart P. An extended privacy calculus model for e-commerce transactions. *Information Systems Research*. 2006; 17(1):61–80.
- Edelman B, Ostrovsky M, Schwarz M. Internet advertising and the generalized second-price auction: selling billions of dollars' worth of keywords. *American Economic Review*. 2007; 97(1):242–259.
- Gandy OH. Public opinion surveys and the formation of privacy policy. *Journal of Social Issues*. 2003; 59(2):283–299.
- Graeff TR, Harmon S. Collecting and using personal data: consumers' awareness and concerns,'. *Journal of Consumer Marketing*. 2002; 19(4):302–318.
- Hann I-H, Hui K-L, Lee S-YT, Pong IPL. Overcoming online information privacy concerns: an information-processing theory approach. *Journal of Management Information Systems*. 2007; 24(2):13–42.
- Hansen M. User-controlled identity management: the key to the future of privacy? *International Journal of Intellectual Property Management*. 2008; 2(4):325–344.
- Hong W, Thong J. Internet privacy concerns: an integrated conceptualization and four empirical studies. *MIS Quarterly*. 2013; 37(1):275–298.
- Huberman BA, Adar E, Fine LR. Valuating privacy. *IEEE Security and Privacy*. 2005; 3(5):22–25.
- Jamal A, Coughlan J, Kamal M. Mining social network data for personalisation and privacy concerns: a case study of Facebook's Beacon. *International Journal of Business Information Systems*. 2013; 13(2):173–198.
- Jenitzsch, N.; Preibusch, S.; Harasser, A. An Economic Model for Pricing Personal Information. *European Network and Information Security Agency (ENISA)*; 2012. Study on Monetising Privacy. Deliverable 2012-02-27

- Jensen C, Potts C, Jensen C. Privacy practices of internet users: self-reports versus observed behavior. *International Journal of Human-Computer Studies*. 2005; 63(1–2):203–227.
- Keith MJ, Thompson S, Hale J, Lowry PB. Information disclosure on mobile devices: re-examining privacy calculus with actual user behavior. *International Journal of Human-Computer Studies*. 2013; 71(12):1163–1173.
- Krohn F, Luo X, Hsu MK. Information privacy and online behaviors. *Journal of Internet Commerce*. 2002; 1(4):55–69.
- Kumaraguru, P.; Cranor, L. Privacy Indexes: A Survey of Westin's Studies. 2005 Dec. ISRI Technical Report, CMU-ISR-5-138
- Kutner, MH.; Nachtsheim, CJ.; Neter, J.; Li, W. *Applied Linear Statistical Models*. 5. McGraw-Hill/Irwin; New York: 2005.
- Laufer RS, Wolfe M. Privacy as a concept and a social issue: a multidimensional development theory. *Journal of Social Issues*. 1977; 33(3):22–42.
- Leslie KJ, Acquisti A, Loewenstein G. Strangers on a plane: Context-dependent willingness to divulge sensitive information. *Journal of Consumer Research*. 2011; 37(5):858–873.
- Lewis K, Kaufman J, Christakis N. The taste for privacy: an analysis of college student privacy settings in an online social network. *Journal of Computer-Mediated Communication*. 2008; 14(1):79–100.
- Li X-B, Sarkar S. Class restricted clustering and micro-perturbation for data privacy. *Management Science*. 2013; 59(4):796–812.
- Li X-B, Sarkar S. Digression and value concatenation to enable privacy-preserving regression. *MIS Quarterly*. 2014; 38(3):679–698. [PubMed: 26752802]
- Li Y. Theories in online information privacy research: a critical review and an integrated framework. *Decision Support Systems*. 2012; 54(1):471–481.
- Malhotra NK, Kim SS, Agarwal J. Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model. *Information Systems Research*. 2004; 15(4):336–355.
- Motiwalla L, Li X-B. Developing privacy solutions for sharing and analysing healthcare data. *International Journal of Business Information Systems*. 2013; 13(2):199–216.
- Norberg PA, Horne DR, Horne DA. The privacy paradox: personal information disclosure intentions versus behaviors. *The Journal of Consumer Affairs*. 2007; 41(1):100–126.
- Preibusch S. Guide to measuring privacy concern: review of survey and observational instruments. *International Journal of Human-Computer Studies*. 2013; 71(12):1133–1143.
- Schreiner, M.; Thomas, H. On the willingness to pay for privacy as a freemium model: First empirical evidence. *Proceedings of the 21st European Conference on Information Systems*; Atlanta, USA: Association for Information Systems; 2013.
- Smith HJ, Dinev T, Xu H. Information privacy research: an interdisciplinary review. *MIS Quarterly*. 2011; 35(4):989–1015.
- Smith HJ, Milberg SJ, Burke SJ. Information privacy: measuring individuals' concerns about organizational practices. *MIS Quarterly*. 1996; 20(2):167–196.
- Sutanto J, Palme E, Tan C, Phang CW. Addressing the personalization-privacy paradox: an empirical assessment from a field experiment on smartphone users. *MIS Quarterly*. 2013; 37(4):1141–1164.
- Taddicken M. The 'privacy paradox' in the social web: the impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. *Journal of Computer-Mediated Communication*. 2014; 19(2):248–273.
- Tsai JY, Egelman S, Cranor L, Acquisti A. The effect of online privacy information on purchasing behavior. *Information Systems Research*. 2011; 22(2):254–268.
- Turhan SN, Vayvay O. Vendor managed inventory via SOA in healthcare supply chain management. *International Journal of Business Information Systems*. 2012; 9(4):451–464.
- Varian HR. Position auctions. *International Journal of Industrial Organization*. 2007; 25(6):1163–1178.
- Wang S-C, Wu J-R. Proactive privacy practices in transition: toward ubiquitous services. *Information and Management*. 2014; 51(1):93–103.
- Westin, A. *Privacy and Freedom*. Atheneum; New York: 1967.
- Westin A. Intrusions: privacy tradeoffs in a free society. *Public Perspective*. 2000 Nov-Dec;:8–11.

- Xu H, Luo X, Carroll JM, Rosson MB. The personalization privacy paradox: an exploratory study of decision making process for location-aware marketing. *Decision Support Systems*. 2011; 51(1): 42–52.
- Xu H, Teo HH, Tan BCY, Agarwal R. The role of push-pull technology in privacy calculus: the case of location-based services. *Journal of Management Information Systems*. 2010; 26(3):137–176.

Figure 1.
Research model

Table 1

Demographic statistics of participants

Demographic attributes	Category	Percentage (%)
Gender	Female	51.8
	Male	48.2
Age	18–23	27.9
	24–29	27.4
	30–39	18.6
	40–49	13.7
	50 and over	12.3
Race	African American	5.9
	Asian	17.1
	Hispanic	6.9
	White	67.2
	Other	2.9
Marital status	Never married	62.2
	Married	28.4
	Divorced/separated	7.4
	Other	2.0

Table 2

Westin GPC segments price valuations

	Fundamentalist	Pragmatist and unconcerned	Combined
Mean bid price	\$642.00	\$281.48	\$372.44
Standard deviation	705.03	400.12	517.53
Sample size (N)	55	163	218

Table 3

Fundamentalalist vs other groups – mean bid price t-test

Price bid	t	df	Signif. (two-tailed)	Mean difference	Std. error difference
Equal variances assumed	4.677	216	.000	360.521	77.081
Equal variances not assumed	3.602	66	.001	360.521	100.099

Table 4

List of independent variables and survey questions with scale

Category	Variable name		Corresponding survey questions with scale
GPC	GPC1	1	Consumers have lost all control over how personal information is collected and used by companies. [5 = 'strongly agree', 4 = 'somewhat agree', 3 = 'not sure', 2 = 'somewhat disagree', 1 = 'strongly disagree']
	GPC2	2	Most businesses handle the personal information they collect about consumers in a proper and confidential way. [5 = 'strongly agree', 4 = 'somewhat agree', 3 = 'not sure', 2 = 'somewhat disagree', 1 = 'strongly disagree']
	GPC3	3	Existing laws and organisational practices provide a reasonable level of protection for consumer privacy today. [5 = 'strongly agree', 4 = 'somewhat agree', 3 = 'not sure', 2 = 'somewhat disagree', 1 = 'strongly disagree']
IDC	IDC1	4	Sharing my data will help me access better products and services. [5 = 'strongly agree', 4 = 'somewhat agree', 3 = 'not sure', 2 = 'somewhat disagree', 1 = 'strongly disagree']
	IDC2	5	Sharing my data will make me more vulnerable to identity theft. [5 = 'strongly agree', 4 = 'somewhat agree', 3 = 'not sure', 2 = 'somewhat disagree', 1 = 'strongly disagree']
	IDC3	6	I am willing to share my data if I know and trust the data collector or website. [5 = 'strongly agree', 4 = 'somewhat agree', 3 = 'not sure', 2 = 'somewhat disagree', 1 = 'strongly disagree']
	IDC4	7	I am more concerned about privacy of my personal information given over the internet compared with telephone, fax or mail. [5 = 'strongly agree', 4 = 'somewhat agree', 3 = 'not sure', 2 = 'somewhat disagree', 1 = 'strongly disagree']
PDB	PDB1	8	How often do you sign the consent form to authorise the doctor and the affiliated medical institution to share your medical information with other doctors and institutions? [5 = 'never', 2 = 'often', 3 = 'don't remember', 4 = 'not often', 1 = 'always']
	PDB2	9	How often do you share your salary information (or grade information for student) with your friends? [5 = 'never', 2 = 'often', 3 = 'don't remember', 4 = 'not often', 1 = 'always']
	PDB3	10	How frequently do you enter your full name in Google or other search engines? [5 = 'never', 2 = 'often', 3 = 'don't remember', 4 = 'not often', 1 = 'always']
	PDB4	11	On Facebook, I share my status updates, posts and photos with_____ [5 = 'nobody', 4 = 'friend-of-friends', 3 = 'do not use', 2 = 'friends', 1 = 'public']
	PDB5	12	I generally share location information on my mobile device with_____ [5 = 'nobody', 4 = 'GPS only', 3 = 'do not use', 2 = 'Wi-Fi and cell tower', 1 = 'all apps']
	PDB6	13	On Twitter, my privacy setting allows_____ [5 = 'location detection', 4 = 'others to find me', 3 = 'do not use', 2 = 'protected use', 1 = 'public tweets']

Table 5

Data analysis on independent variables

Variable name	Description	Mean (scale = 5)	Std. deviation	Strongly agree/somewhat agree	Not sure	Strongly disagree/somewhat disagree
GPC1	Lost all control of PI	4.03	.955	81.2%	9.6%	9.2%
GPC2	PI collected and handled properly	2.94	1.097	35.3%	25.2%	39.4%
GPC3	Laws and practices protect PI	2.88	1.101	34.8%	23.4%	41.7%
IDC1	Sharing data provides better access	2.94	1.124	35.8%	30.3%	33.9%
IDC2	Sharing data increases risks	4.22	.889	83.0%	11.5%	5.5%
IDC3	Willing to share if trusted firm	3.86	1.100	73.4%	13.3%	13.3%
IDC4	Higher privacy concerns on internet	3.34	1.290	51.0%	15.1%	33.9%
PDB1	Share health data with medical providers	2.601	1.2374	48.2%	27.1%	24.8%
PDB2	Share salary or grade info with friends	3.399	1.3290	33.9%	5.0%	61.0%
PDB3	Enter PI on search engines	3.427	1.1646	29.8%	11.5%	58.7%
PDB4	Share info on Facebook	3.58	.948	15.6%	11%	73.4%
PDB5	Share location info on mobiles	3.38	1.407	26.6%	16.5%	56.9%
PDB6	Privacy settings on Twitter	2.67	.887	N/A *	58.7%	N/A *

Note:

* Majority of users were not Twitter users and did not have good sample distribution.

Table 6

Results of regression analysis

Independent variables	Coefficients (p-value)	Expected direction of relationship with dependent variable
GPC1	+0.7195 (0.3939)	+
GPC2	-0.9382 (0.2333)	-
GPC3	-0.4748 (0.5731)	-
IDC1	+0.0949 (0.8945)	-
IDC2	+1.0970 (0.2281)	+
IDC3	-0.5654 (0.4196)	-
IDC4	-0.8329 (0.1406)	+
PDB1	+0.9925 (0.0989)	+
PDB2	+1.3715 (0.0162)	+
PDB3	+0.2913 (0.6428)	+
PDB4	+1.4791 (0.0622)	+
PDB5	-0.5566 (0.3018)	+
PDB6	-1.4582 (0.0825)	+
$R^2 = 0.1672$		