Re-examining the Privacy Paradox Through Cognitive Neuroscience Perspective

Full Paper

Zareef A. Mohammed
Nova Southeastern University
zm58@nova.edu

Gurvirender P. Tejay
Nova Southeastern University
tejay@nova.edu

Abstract

The concerns individuals express over the privacy of their personal information could inhibit them from disclosing their personal information, despite the benefits they may attain from doing so. However, while individuals' express privacy concerns, they still continue to disclose personal information. The actions of such individuals, known as the privacy paradox, suggests that there are factors are present which may influence or inhibit individuals from disclosing personal information. The aim of our study is to investigate the privacy paradox to better understand individuals' decisions to withhold or disclose personal information. We argue that individuals disclose personal information based on a cognitive disposition, which includes rational and emotional mental processes. We further posit that by adopting techniques, tools and theories from the cognitive neuroscience will help us better understand the privacy paradox.

Keywords

Privacy paradox, privacy calculus, cognitive neuroscience.

Introduction

Even though organizations and individuals can capitalize on the benefits provided by the internet whereby personal information can be exchanged, there exist growing concerns of information privacy within these exchanges (Madden et al., 2007; Smith et al., 2011). Information privacy is regarded as a human right (Solove 2006) and as such, inhibits the disclosure of personal information (Dinev and Hart 2006; Malhotra et al., 2004). For instance, a key component of e-commerce is the use of consumers' personal information to provide better services (Culnan and Armstrong 1999). However, while e-commerce sales in the US increased by 4% in the third quarter of 2014 (US Censor News, 2014), it still represented only 6.6% of total retail sales. Extant literature has found that privacy concerns were an impediment to e-commerce adoption (Dinev and Hart 2006; Li et al., 2011).

E-health faces a similar problem as e-commerce, whereby patients are concerned over their personal medical records (Bishop et al., 2005). However, the benefits and consequences in the adoption of e-health are more serious as it is involved with human lives. Governments such as those of the US and United Kingdom, have invested in e-health as a means of fostering safer and more efficient healthcare systems (Angst and Agarwal 2009). E-health essentially connects doctors and hospitals to reduce medical errors and high administrative costs (Bates and Gawande 2003; Becker 2004), which leads to a greater probability of human lives being saved. Yet, despite the tremendous benefits that could revolutionize the healthcare industry through the investment and adoption of e-health, it becomes a significant problem if patients withhold personal information due to privacy concerns. Researchers have found, that while privacy concerns remain a constant inhibitor to disclosing personal information, there exists a privacy paradox. The privacy paradox occurs when individuals express concern for their information privacy, yet act contrarily by disclosing personal information (Dinev and Hart 2006; Smith et al., 2011). The objective of our study is to investigate the privacy paradox to better understand individuals' decisions to withhold or disclose personally identifiable information.

Prior literature has argued that trust plays an important role in the moderation of privacy concerns (Pavlou et al., 2007) and in directly disclosing personal information (Belanger et al., 2002). Similarly, Dinev and Hart (2006) argued that trust is only one factor in a set of contrary salient factors which form a rational cost-benefit analysis individuals undergo before providing personal information. However, Acquisti (2004) stated that it is nearly impossible for individuals to make a perfectly rational decision with regards to information privacy. Individuals are bounded by a lack of knowledge of all parameters when asked to disclose personal information, and even if they did have all the knowledge to make a rational choice, it is impossible to process all of it (Acquisti 2004). Based on the findings of previous studies, we argue that individuals disclose personal information based on a cognitive disposition, which includes rational and emotional mental processes.

Our study aims to contribute to the information privacy area by providing a better understanding of the privacy paradox. To do this, we would employ techniques from the cognitive neuroscience literature. According to Dimoka et al. (2007, 2011), using techniques and theories from the field of cognitive neuroscience could revolutionize the information systems (IS) field, since functional neuroimaging tools could be used to examine actual behavior of individuals under specific situations. Investigating and understanding the privacy paradox is the means by which organizations and individuals could leverage the benefits of technologies that require personal information disclosure.

Information Privacy Supported by Cognitive Neuroscience

Information privacy refers to the ability an individual possesses to control the collection, access and use of his/her personal information (Smith et al., 1996; Westin 1967). Studies have found that while privacy concerns inhibit individuals from disclosing personal information (Culnan and Armstrong 1999; Dinev and Hart 2006), the existence of the privacy paradox indicates that privacy concerns could be subverted by other factors that influences individuals' disclosure of personal information. A widely accepted explanation for the privacy paradox is that of the privacy calculus model, whereby individuals would decide to disclose or withhold personal information based on a cost-benefit analysis of salient but contrary factors (Culnan and Armstrong 1999; Dinev and Hart 2004, 2006). As such, the privacy calculus assumes that individuals would make rational decisions with regards to the privacy of their personal information.

Despite the findings of the privacy calculus as a strong explanation to the privacy paradox (Dinev and Hart 2004, 2006), Acquisti and Grossklags (2005) debated that individuals' privacy decisions are not purely rational but subject to incomplete knowledge, bounded rationality and psychological deviation. Within any decision an individual makes, there are a full range of cognitive abilities that must be considered. Essentially, this includes both rational choices and emotional choices. It may be possible that individuals would disclose personal information, despite the fact that costs are higher than the benefits, which would explain the findings of Belanger et al. (2002), where individuals were less concerned about their information security and privacy when considering pleasure features in online transactions. Furthermore, considering both the rationality and emotional interactions within the decision to disclose personal information could explain the findings of Norberg et al. (2007) whereby individuals' actual disclosure of personal information exceeded their intentions.

The insights of cognitive neuroscience could deliver a better understanding of the privacy paradox by examining how the cognitive abilities of an individual influence his/her decision to disclose or withhold personal information. The cognitive neuroscience field uses functional neuroimaging tools to measure the brain activation in response to mental processes. Essentially, applying cognitive neuroscience to the social sciences could radically advance research pursuits (Dimoka et al., 2007). With regards to the privacy paradox, cognitive neuroscience could map individuals' mental processes to their associated brain activity, thereby gaining a better insight into individuals' privacy beliefs.

The human brain is comprised of specific areas which regulates the decision-making, rational, emotional and social processes of each individual (Dimoka et al., 2011). There are two major areas of the brain related to individuals' decision-making, which are the prefrontal cortex and the limbic system (Dimoka et al., 2007; 2011). The prefrontal cortex is responsible for cognitive and social processes such as problem solving, calculation, thinking and goals, while the limbic system is related to individuals' emotions (Dimoka et al., 2011). Yet, despite the separation of the brain areas for rational and emotional processes, both the prefrontal cortex and limbic system often interact with each other (Phelps 2006). This

suggests that no decision may be purely rational or emotional, and as such, there is a high degree of complexity involved in decision-making.

Research in the area of the privacy paradox has often identified mental processes such as individuals' assessment of risk and trust as influential factors to individuals' decision to withhold or disclose personal information (Dinev and Hart 2006; Norberg et al., 2007; Smith et al., 2011; Van Slyke et al., 2006). Particularly, Dinev and Hart (2006) introduced the extended privacy calculus model that found risk, trust, privacy concerns and personal interest as salient in the individuals' decisions to disclose their personal information. By applying the findings from cognitive neuroscience, the nature of these mental processes could be better understood with regards to their relationship to personal information disclosure. The integration of cognitive neuroscience with information privacy could advance IS field by "localizing the brain areas which are associated with IS constructs, capture hidden processes, compliment existing sources of data, identify antecedents to IS constructs, compliment existing sources of data, infer causality and challenge IS assumptions" (Dimoka et al., 2007, p. 688). Since intentions may not accurately predict individuals' actual behavior (Smith et al., 2011); the use of cognitive neuroscience tools and techniques for experimentation could lead to more accurate findings for individuals' actual privacy related behavior.

Privacy Calculus

Dinev and Hart (2006) argued that individuals would make an assessment of the costs and benefits of disclosing their personal information. Essentially, contrary but salient factors of risk beliefs (privacy risk and privacy concerns) and confidence and enticement beliefs (trust and personal interest) would form the basis for individuals' behavior, which was determined by which set of beliefs outweighed the other (Dinev and Hart 2006). The factors identified by Dinev and Hart (2006) corroborates with the findings of other privacy studies. For instance, privacy risk has been found by Malhotra et al. (2004) and Norberg et al. (2007) as inhibitors of individuals' disclosure of personal information. Similarly, privacy concerns are used as a measure of privacy (Smith et al., 2011), and have been found to both directly and indirectly inhibit personal information disclosure (Angst and Agarwal 2009; Bansal et al., 2010; Pavlou et al. 2007; Van Slyke et al., 2006). Both privacy concerns and privacy risk were considered as risk beliefs in the extended privacy calculus model (see Figure 1) proposed by Dinev and Hart (2006).

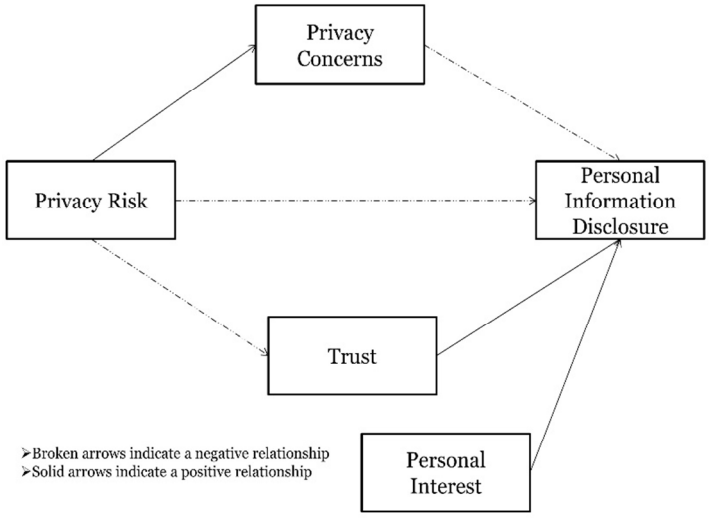

Figure 1. Extended Privacy Calculus Model

Confidence and enticement beliefs are composed of trust and personal interest. Dinev and Hart (2006) found both factors to be significant in influencing individuals' personal information disclosure. This is consistent with the stream of research arguing that trust is necessary in privacy decisions (Smith et al., 2011). Individuals' trust in organizations would significantly influence them to disclose personal

information (Lin and Wu 2008; Liu et al., 2005; Malhotra et al., 2004). Likewise, trust could act as a mitigator of privacy concerns (Belanger et al., 2002; Pavlou et al., 2007). Personal interest could explain with the findings of Belanger et al. (2002) that in the presence of pleasure features, security and privacy are less important to individuals. As such, the findings of the extended privacy calculus provides a strong explanation for the privacy paradox.

Research Model

The extended privacy calculus (Dinev and Hart 2006) forms the basis for our research model. However, as researchers have challenged the assumption that privacy behavior is purely rational (Acquisti 2004; Acquisti and Grossklags 2005), we also present findings from cognitive neuroscience that the privacy calculus is limited in explaining the privacy paradox. The privacy calculus assumes *privacy risk* is a one-dimensional construct which increases privacy concerns, while inhibiting individuals' willingness to transact online, and negatively affecting trust (Dinev and Hart 2006). Yet, an individual's perception of risk may assess the likelihood and severity of negative consequences (Peter and Tarpey 1975). Also, privacy risk was defined as the possibility of loss (see Table 1), which is related to the uncertainty caused by the possibility of harm to the individual if they were to disclose personal information (Dinev and Hart 2006). Yet, findings in cognitive neuroscience have explained that risk may be multi-dimensional as there are different brain activations, based on different situations. The nucleus accumbens, which is primarily attributed to the anticipation of rewards (Knuston et al., 2001), is activated when individuals sought to avoid risky behavior (Matthews et al., 2004). Paulus and Frank (2003) found brain activity in the insular cortex was activated in risky games whereby there were high loss predictions. However, *uncertainty* correlates with the orbitofrontal cortex and the inferior parietal cortices (Krain et al., 2006). While Pavlou et al. (2007) found privacy concerns influenced individual's perceived uncertainty, it is also possible that because of uncertain situations, an individual's privacy concerns are heightened. Similarly, uncertainty would strengthen the level of privacy risk an individual perceives when asked to disclose personal information.

Constructs	Definition	Supporting Literature
Distrust	Strong negative emotions associated with malevolence and discredibility	Dimoka 2010; McKnight and Chervany 2000
Uncertainty	Perceptions based on lack of information pertaining to organization's privacy practices	Dimoka et al. 2007; Pavlou et al., 2007
Risk	Possibility of loss; the benefits of avoiding risky action	Dinev and Hart 2006, Peter and Tarpey 1975
Privacy Concern	Concerns about the collection and use of the personal information an organization collects from an individual	Dinev and Hart 2006; Westin 1967
Trust	Confidence that organizations would act benevolently in protecting indivivudals from harm caused from the personal information they collect	Dinev and Hart 2006
Personal Interest	Intrinsic interest towards content that requires disclosure of personal information	Dinev and Hart 2006

Table 1. Constructs for Research Model

While the privacy calculus found *trust* to be a salient factor (Dinev and Hart 2006), and a positive influence for individual's disclosure of personal information, an important factor of *distrust* was

neglected. Researchers in the social sciences has often assumed trust and distrust existed on opposite ends of the same continuum, and as such, the more trust an individual had, the lesser the degree of distrust (Dimoka 2010). Yet, Dimoka (2010) found that trust activated the caudate nucleus and putamen, while distrust activated the amygdala and insular cortex. This suggests that distrust and trust were separate constructs. Furthermore, Dimoka (2010) found that distrust was a more salient factor as the brain activations of the amygdala was related to strong negative emotions. As such, if an individual was asked to disclose personal information, the distrust he/she would feel for an organization would influence his/her privacy concerns. Yet, as is consistent with the findings of multiple researchers, trust could influence individuals to disclose their personal information (Dinev and Hart 2006, Van Slyke et al., 2006).

In the privacy calculus, *personal interest* was defined as an enticement that would influence individuals to disclose personal information (Dinev and Hart 2006). Personal interest may be derived from the pleasurable and beneficial features that e-commerce or e-health may offer. Despite privacy concerns, individuals may feel that providing personal information to attain the associated benefits would outweigh any privacy concerns. This decision may not be altogether rational, but rather impulsive. As such, consistent with the findings that personal interest or the presence of benefits could outweigh privacy concerns (Belanger et al., 2002; Dinev and Hart 2004), personal interest may be involved with the same cognitive processes as consumer behavior, whereby there is high activations in the ventromedial prefrontal cortex, but low activations in the dorsolateral prefrontal cortex (Deppe et al., 2005).

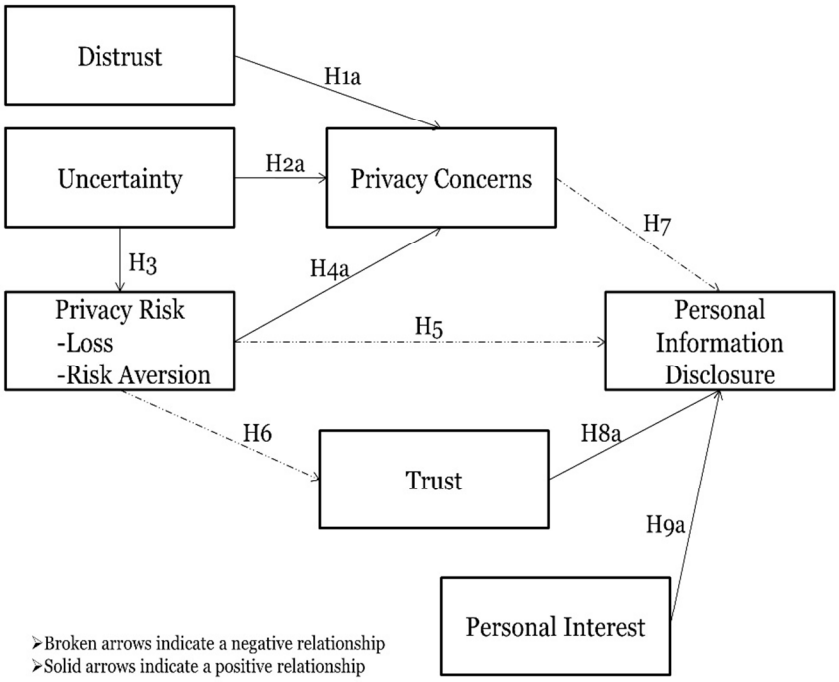

Figure 2. Proposed Research Model Based on Privacy Calculus

Figure 2 depicts our research model when the findings of cognitive neuroscience have been integrated with the extended privacy calculus model. The findings of cognitive neuroscience address the limitations of the privacy calculus, which lead to enhancing the assumptions of the privacy calculus. Specifically, because the factors of the model could be mapped to specific brain areas that carry out different functions, some of which may be rational and others as emotional, the assumption that there exists a cost-benefit analysis in privacy decision-making is limited. Also, as indicated by the findings of cognitive neuroscience, traditional assumptions such as uncertainty being a part of the concept of risk, or trust and distrust as the same construct on opposite ends of a continuum are erroneous. Applying the

findings of cognitive neuroscience to the privacy calculus helps to clarify the limitations of the model, as well as depict a better model to be further tested in solving the privacy paradox phenomonon. A list of hypotheses for future research has been presented in the appendix. The hypotheses directly related to neuroscience aspects were purposely excluded from research model. These hypotheses are related to brain activity to be captured using a functional magnetic resonance imaging (fMRI) device.

Research Design

Research within the field of information privacy has often employed a number of methods, whereby individuals voice their concerns of the privacy of their personal information. However, opportunities now exist which could enrich the information privacy field, through the use of cognitive neuroscience. While prior studies have often used self-reported data such as surveys, interviews and experiments, the tools and techniques of cognitive neuroscience could provide more accurate results. Specifically, since individuals' decision-making are subject to mental processes, it is more logical to directly measure an individuals' brain activity and other physiological features, than using self-reported data. Much of self-reported data is subject to lack of knowledge and bias (Dimoka 2010). For instance, an individual may fail to accurately answer psychometric measures in a given situation because they may be unaware of what drove them to specific decisions. However, directly measuring neural activity or physiological functions could produce more objective and generalized findings, thereby enhancing the information privacy field.

The functional magnetic resonance imaging (fMRI) scanner is one such tool from the cognitive neuroscience realm, whichcould be used to advance privacy research, particularly, the privacy paradox. The fMRI scanner tracks blood oxygenation in the brain and measures the magnetic properties of oxygenated and deoxygenated blood (Riedl et al., 2010). Researchers could thus see individuals' brain activity associated with various situations, thereby relating the factors that influence decision-making due to the spatial resolution from fMRI scans (Riedl et al., 2010). For this reason, the fMRI is the best suited tool for testing the research model and hypotheses of our study. Dimoka (2012) indicated that a sample size of 11-12 subjects were suitable for studies involving fMRI experiments, where $p < 0.05$ (95% confidence interval). Similarly, Dimoka (2010) used 15 participants in studying the effect of trust and distrust on price premiums, where the male to female ratio was 9 to 6. As such, our study requires a minimum of 11 subjects, which should have some level of equivalency between the males and females. However, so that we could attain better results and sufficient within-subject power, 20-24 subjects would be more adequate for the experiment. Furthermore, subjects must all be right-handed so that the results of the experiment would be consistent and not varied due to differences in the handedness of individuals (Dimoka 2012). Subjects can only participate in the experiment provided that their medical history verifies that there are no use of psychotropic medications, no psychological problems, no medical implants, and either normal or corrected-normal visual acuity (Dimoka 2010, 2012).

Hypotheses would be tested based on various feedback profiles, reflecting the constructs of the research model, whereby subjects would be exposed to these profiles, and brain activity would be recorded accordingly (Dimoka 2010). Pavlou and Dimoka (2006) found feedback text comments were good treatments for collecting data since it helps buyers to accept or reject sellers. Since our study does not specifically examine e-commerce or e-health, but is interested in understanding the influencers and inhibitors of individual's decisions to withhold or disclose personal information, feedback profiles would reflect various situations such as online profiling, online transacting and electronic patient records. Feedback profiles would mimic real organizations representing e-commerce and e-health to elicit responses from subjects as have been done in past studies (Ba and Pavlou 2002; Dimoka 2010). Subjects would be given the profiles a day before experimentation so that they could familiarize and analyze them, thus reducing the time they would need to process a mental response during experimentation. Twenty-four hours is sufficient for subjects to internalize the profiles as it is not too long a time for them to forget, nor too short for them to hurriedly read the profiles. Following the method of Dimoka (2010), subjects would be screened to ensure they pass the criteria for participation, and placed in the fMRI scanner, where they will be shown digital projections of the feedback profiles. Since subjects are expected to be familiar with the profiles, each profile would be displayed for a 5 second window, before they are asked whether they would disclose personal information or not. This is consistent with the approach of Dimoka (2010) whereby subjects were given a 3 second window before answering measurement items. The measurement items would ask individuals whether they would disclose their personal information or not,

where they would click one button on a fiber-optic device to give their approval, and the second button if they reject.

Profiles 1 would reflect a high degree of distrust such as organization's opportunistic behavior with client's personal information, whereas profile 2 would reflect a high degree of uncertainty (i.e. profiles would be ambiguous and incomprehensive privacy policies would be mentioned). Profile 3 would reflect a high degree of risk to individuals' personal information, such as feedback indicating past data breaches, and high loss of clients' personal information. Profile 4 would reflect a high degree of trust with regards to information privacy, such as comprehensive privacy policies, good privacy practices and transparency in use of clients' personal information. Therefore, profiles 1 to 4 would test the presence of the constructs within our research model, and their relationship towards privacy concerns and individuals decisions to withhold or disclose personal information. However, subjects would be given a number of other profiles, whereby each profile would represent some combination of a high-low matrix of each construct. For example, profile 5 would reflect a high degree of trust, a high degree of privacy risk, and similarly, a high degree of uncertainty and distrust. Yet, profile 6 would reflect a low degree of trust with high degrees of privacy risk, uncertainty and distrust. This approach is consistent with that of Dimoka (2010), where seller profiles had a 2x2 matrix of high and low trust and distrust combinations. As such, the interactions and saliency of constructs would be highlighted, thus explaining the nature of the privacy paradox. Personal interest would require testing where the context of individuals' decisions are different. Therefore, profiles would reflect high degrees of privacy concerns, yet subjects would be asked to purchase a specific product online, or disclose their medical history. As such, the treatment would simulate the situation whereby an individual's needs and/or wants are pitted against his/her privacy concerns.

Between each profile displayed to the subjects, a control treatment would be required whereby subjects would be asked to click any button on the fiber-optic device. This is so that any neural activity of the past treatment does not interfere with the next treatment, since this is a within-subject experiment (Dimoka 2010). Due to the constraints of an fMRI scanner, subjects are not allowed to move and should remain still since bodily motions could affect the outcome of brain activity (Dimoka 2012). As such, each subject should ideally be tested for 30 minutes so as to not cause fatigue and distress to the subject (Dimoka 2012). The use of a neuroscience tool such as the fMRI to test the relationships and nature of the constructs in our research model would essentially address the limitation of the privacy calculus' base assumptions. Subsequently, this would lead to better understanding of the privacy paradox.

Discussion

Mason (1986) predicted that privacy would be a major issue with the increased use and evolution of information technology. Information privacy has become a topic of debate for practitioners, political debates, and societal infrastructure. Researchers have endeavored to understand the concept of information privacy, yet has still not fully articulated its meaning (Solove 2006). Interestingly, research has indicated the presence of the privacy paradox, whereby individuals claim to have high privacy concerns, yet continue to disclose their personal information in varied situations such as online transactions and profiling (Dinev and Hart 2006; Norberg et al., 2007; Smith et al., 2011). The privacy calculus was found to be a worthy explanation for the privacy paradox, and has been adopted and extended by multiple researchers in their investigations in the privacy field (Dinev and Hart 2004, 2006; Li et al., 2011; Xu et al., 2010). The privacy calculus assumed that rationally, individuals would undergo a calculation of costs versus benefits. Yet, a stream of research has found that privacy decisions are not purely rational (Acquisti 2004; Acquisti and Grossklags 2005; Anderson and Agarwal 2011; Li et al., 2011).

The review of privacy literature has revealed the factors identified by Dinev and Hart (2006) as salient in determining individuals' privacy-related decisions. However, findings from cognitive neuroscience have indicated that the assumptions of the nature and relationships of these factors (which consists of trust and personal interest defined as confidence and enticement beliefs, and risk and privacy concerns defined as risk beliefs), can be challenged. Findings from cognitive neuroscience have explained that mental processes are correlated with activity in specific brain areas (Dimoka et al., 2007). In essence, the mental processes involved in individuals' decision making are distinct from one another. The findings from cognitive neuroscience emphasize the importance of including uncertainty and distrust in the privacy calculus. Furthermore, privacy risk is a multidimensional factor, in that it consists of an

individuals' perception of loss and risk aversion. This indicates that our theoretical understanding of the privacy paradox requires revision for the advancement of knowledge in privacy research.

Privacy research often uses psychometric measures of self-reported data, which are often limited due to individuals' biases (Dimoka et al., 2007, 2010). However, directly measuring individuals' neural activity and/or physiological features provides more accurate and objective data (Riedl et al., 2010). While Smith et al. (2011) indicated that limited insights could be gained from testing research models of perceptions, the tools and techniques of cognitive neuroscience could overcome these constraints, particularly in privacy research. It is imperative to consider individuals' perceptions in order to elicit a thorough understanding of information privacy.

Implications for Practice

Information privacy is a societal issue whereby individuals' are vulnerable when they disclose their personal information. These privacy issues often lead to limiting the benefits information systems have to offer. Likewise, organizations could better serve individuals through the collection and use of their personal information. Furthermore, organizations require individuals' personal information to be competitive (Culnan and Armstrong 1999). However, organizations should follow basic privacy principles in this exchange of personal information. This could in turn lead individuals to disclose their personal information. Table 2 provides the privacy principles to address critical cognitive factors of distrust and uncertainty.

Critical Cognitive Factors	Privacy Principles	Recommended Organizational Privacy Practices
Distrust	Reduce negative outcomes of personal information disclosure	1. Adhere to obligatory regulations to protect collected personal information 2. Implement additional strategies that goes beyond obligations in protecting collected personal information
	Beneficence towards preserving information privacy	1. Create comprehensive privacy policies 2. Inform individuals of the organization's protection strategies of collected personal information 3. Help individuals overcome privacy incidents
Uncertainty	Provide transparency of privacy practices	1. Give individuals control of their personal information 2. Accreditation of privacy practices by third-party authorities 3. Create a virtual social presence

Table 2. Information Privacy Principles to Address Critical Cognitive Factors

Based on the findings of cognitive neuroscience, organizations should focus on accentuating the positive beliefs of an individual's privacy assessment, while avoiding and relieving their negative beliefs. Studies have often discussed the implications of trust, in that organizations should try to build good relationships with individuals while offering them control over their personal information (Lin and Wu 2008; Malhotra et al., 2004). Similarly, organizations should aim to build relationships with individuals who are more willing to disclose their personal information, while offering them valuable products and services (Awad and Krishnan 2006). Yet, organizations also need to minimize the negative consequences arising from factors of distrust, uncertainty; especially since research has found negative outcomes to be

more critical to individuals in their decision-making processes (Dimoka 2010; Kahneman and Tversky 1979). To address individuals' perceptions of privacy risk, privacy concern, uncertainty and distrust, organizations should adhere to the following principles: (1) reduce negative outcomes of personal information disclosure, (2) beneficence towards preserving information privacy, and (3) provide transparency of privacy practices.

An individual's distrust is influenced by perceptions of an organization's discredibility and malevolence (Dimoka 2010; McKnight and Chervany 2000). Therefore, organizations should aim to reduce negative outcomes of personal information disclosure. Mandatory regulations are initial steps towards adequately safeguarding personal information, however, organizations' information protection strategies should surpass obligations. Employing strategies to better safeguard collected personal information reduces the probability of privacy and security incidents. By doing so, organizations could avoid negative reputation.

Organizations should seek to highlight positive posture to information privacy. In order to do so, organizations should have a duty of beneficence towards protecting individuals from harm due to compromises to their personal information. This is particularly the case when we have knowledge or awareness of such a compromise, and possess the capability to provide assistance. Further, organizations should develop comprehensive privacy policies informing individuals of how personal information is collected and used. However, while organizations are required to notify individuals when their personal information is compromised, beneficence is reflected when organizations further help individuals to overcome the privacy incidents. This can be done by ways of assistance programs or compensation packages. By exhibiting moral responsibility towards personal information, individuals would perceive organizational actions as sincere and trustworthy. Essentially, the above discussed privacy principles will reduce the distrust towards organizational privacy practices.

Organizations should provide transparency with respect to their privacy practices. Individuals are often unaware of the organizations' activities since they cannot continually monitor their practices (Pavlou et al., 2007). Yet, organizations could mitigate this uncertainty by explicitly informing individuals how they collect and use personal information (Awad and Krishnan 2006). In addition, organizations should provide their individuals control over their personal information. For instance, individuals should be allowed to edit the information collected about them, as well as opt-out of organization-client relationships (Malhotra et al., 2004). Furthermore, organizations should subject themselves to accreditation of good privacy practices to third-party authorities, which would assure individuals that the organization's privacy practices are adequate (Pavlou et al., 2007). Finally, organizations should create and maintain a virtual social presence (Pavlou et al., 2007). At the minimum, individuals should have some effective means of communicating with organizations.

Conclusion

Information privacy is a topic of concern for individuals and an impediment when they are asked to disclose their personal information to organizations. Yet, the disclosure of personal information can greatly benefit individuals with regards to e-commerce and especially, e-health. As such, it becomes important to explore the privacy paradox, whereby individuals would claim privacy concerns, yet act contrarily. Thus, investigating the privacy paradox would help individuals and organizations to leverage the benefits of e-commerce and e-health. Studying the privacy paradox from a cognitive disposition has the potential to achieve a better understanding of the phenomenon, since individuals' decision-making are not purely rational or emotional, but a combination of both.

The insights from the cognitive neuroscience literature provides a means of achieving the objectives of our study. Specifically, the use of fMRI would allow us to map the mental processes of individuals when asked to disclose personal information to specific brain areas. Subsequently, we would seek to collect data on individual's actual behavior when asked to provide personal information. The potential contribution is to provide a better understanding of the privacy paradox by extending the privacy calculus supported by findings of cognitive neuroscience literature.

References

Acquisti, A. 2004. "Privacy in Electronic Commerce and the Economics of Immediate Gratification," *Proceedings of the 5th ACM Electronic Commerce Conference*, pp. 21-29.

Acquisti, A. and Grossklags, J. 2005. "Privacy and Rationality in Individual Decision Making," *IEEE Security & Privacy* (3:1), pp. 26-33.

Anderson, C. L., and Agarwal, R. 2011. "The Digitization of Healthcare: Boundary Risks, Emotion, and Consumer Willingness to Disclose Personal Health Information," *Information Systems Research* (22: 3), pp. 469-490.

Angst, C. M., and Agarwal, R. 2009. "Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion," *MIS Quarterly* (33:2), pp. 339-370.

Awad, N. F., and Krishnan, M. S. 2006. "The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to be Profiled for Online Personalization," *MIS Quarterly* (30:1), pp. 13-28.

Ba, S., and Pavlou, P. A. 2002. "Evidence of the Effect of Trust in Electronic Markets: Price Premiums and Buyer Behavior," *MIS Quarterly* (26:3), pp. 243-267.

Bansal G., Zahedi, F. M., and Gefen, D. 2010. "The Impact of Personal Dispositions on Information Sensitivity, Privacy Concern and Trust in Disclosing Health Information Online," *Decision Support Systems* (49), pp. 138-150.

Bates, D. W., and Gawande, A. 2003. "Improving Safety with Information Technology," *New England Journal of Medicine* (348), pp. 2526-2534.

Becker, C. 2004. "The Best Care Money Can Buy?," *Modern Healthcare.com*, August 9 (http://www.modernhealthcare.com/apps/pbcs.dll/article?AID=/20040809/REG/408090324&nochache=1).

Belanger, F., and Crossler, R. E. 2011. "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems," *MIS Quarterly* (35:4), pp. 1017-1041.

Belanger, F., Hiller, J. S., and Smith, W. J. 2002. "Trustworthiness in Electronic Commerce: The Role of Privacy, Security, and Site Attributes," *Journal of Strategic Information Systems* (11), pp. 245-270.

Bishop, L. S., Holmes, B. J. and Kelley, C. M. 2005. "National Consumer Health Privacy Survery 2005," California HealthCare Foundation, Oakland, CA.

Culnan, M. J., and Armstrong, P. K. 1999. "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation," *Organization Science* (10:1), pp. 104-115.

Deppe, M., Schwindt, W., Kugal, H., Plassman, H., and Kenning, P. 2005. "Nonlinear Responses Within the Medical Prefrontal Cortex Reveal When Specific Implicit Information Influences Economic Decision Making," *Journal of Neuroimaging* (15:2), pp. 171-182.

Dimoka, A. 2010. "What Does the Brain Tell Us About Trust and Distrust? Evidence From a Functional Neuroimaging Study," *MIS Quarterly* (34:2), pp. 373-396.

Dimoka, A. 2012. "How To Conduct A Functional Magnetic Resonance (FMRI) Study in Social Science Research," *MIS Quartely* (36:3), pp. 811-840.

Dimoka, A., Pavlou, P. A., and Davis, F. D. 2007. "NeuroIS: The Potential of Cognitive Neuroscience for Information Systems Research," *28th International Conference of Information Systems, Montreal*, pp. 1-20.

Dimoka, A., Pavlou, P. A., and Davis, F. D. 2011. "NeuroIS: The Potential of Cognitive Neuroscience for Information Systems Research," *Information Systems Research* (22:4), pp. 687-702.

Dinev, T. and Hart, P. 2004. "Internet Privacy Concerns and Their Antecedents-Measurement Validity and Regression Model," *Behavioral & Information Technology* (23:6), pp. 413-422.

Dinev, T., and Hart, P. 2006. "An Extended Privacy Calculus Model for E-Commerce Transactions," *Information Systems Research* (17:1), pp. 61-80.

Kahneman, D., and Tversky, A. 1979. "Prospect Theory: An Analysis of Decision under Risk," *Econometrica* (47:2), pp. 263-292.

Kraine, A., Wilson, A. M., Arbuckle, R., Castellanos, F. X., and Milham, M. P. 2006. "Distinct Neural Mechanisms of Risk and Ambiguity: A Meta-Analysis of Decision-Making," *Neuroimaging* (32:1), pp. 477-484.

Knuston, B., Adams, C. M., Fong, G. W., and Homer, D. 2001. "Anticipation of Increasing Monetary Reward Selectively Recruits Nucleus Accumbens," *The Journal of Neuroscience* (21), pp. 1-5.

Li, H., Sarathy, R., and Xu, H. 2011. "The Role of Affect and Cognition on Online' Decision to Disclose Personal Information to Unfamiliar Online Vendors," *Decision Support Systems* (51), pp.434-445.

Lin, Y. and Wu, H. –Y. 2008. "Information Privacy Concerns, Government Involvement, and Corporate Policies in the Customer Relationship Management Context," *Journal of Global Business and Technology* (4:1), pp. 79-91.

Liu, C., Marchewka, J. T., Lu, J., and Yu, C. –S. 2005. "Beyond Concern-a Privacy-Trust-Behavioral Intention Model of Electronic Commerce," *Information & Management* (42), pp. 289-304.

Madden, M., Fox, S., Smith, A., and Vitak, J. 2007. "Digital Footprints: Online Identity Management and Search in the Age of Transparency," (*http://pewresearch.org/pubs/663/digital-footprint* retrieved June 15th, 2014).

Malhotra, N. K., Kim, S. S., and Agarwal, J. 2004. "Internet Users' Information Privacy Concerns (IUIPC): The Construct, Scale, and a Causal Model," *Information Systems Research* (15:4), pp. 336-355.

Margulis, S. T. 1977. "Conceptions of Privacy: Current Status and Next Steps," *Journal of Social Issues* (33:3), pp. 5-21.

Mason, R. O. 1986. "Four Ethical Issues of the Information Age," *MIS Quarterly* (10:1), pp. 5-12.

Matthews, S. C., Simmons, A. N., Lane, S. D., and Paulus, M. P. 2004. "Selective Activation of the Nucleus Accumbens During Risk-Taking Decision Making," *Neuroreport* (15:13), pp. 2123-2127.

McKnight, D. H., and Chervany, N. L. 2000. "While Trust is Cool and Collected, Distrust is Fiery and Frenzied: A Model of Distrust Concepts," in *Proceedings of the 6th Americas Conference on Information Systems,* Long Beach, CA, August 10-13, pp. 883-888.

Norberg, P. A., Horne, D. R., and Horne, D. A. 2007. "The Privacy Paradox: Personal Information Intentions Versus Behavior," *The Journal of Consumer Affairs* (41), pp. 100-126.

Paulus, M. P., and Frank, L. R. 2003. "Ventromedial Prefrontal Cortex Activation is Critical for Preference Judgments," *Neuroreport* (14:10), pp. 1311-1315.

Pavlou, P. A., and Dimoka, D. 2006. "The Nature and Role of Feedback Text Comments in Online Marketplaces: Implications for Trust Building, Price Premiums, and Seller Differentiation," *Information Systems Research* (17:4), pp. 391-412.

Pavlou, P. A., Liang, H., and Xue, Y. 2007. "Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principle-Agent Perspective," *MIS Quarterly* (31:1), pp. 105-136.

Peter, J. P., and Tarpey, S. L. X. 1975. "A Comparative Analysis of Three Consumer Decision Strategies," *Journal of Consumer Research* (2), pp. 29-37.

Phelps, E. A. 2006. "Emotion and Cognition: Insights from Studies of the Human Amygdala," *Annual Review of Psychology* (57), pp. 27-53.

Riedl, R., Banker, R. D., Benbasat, I., Davis, F. D., Dennis, A. R., Dimoka, A.,...Weber, B. 2010. "On the Foundations of NeuroIS: Reflections on the Gmunden Retreat 2009," *Communications of the Association for Information Systems* (27:15), pp. 243-264.

Smith, H. J., Dinev, T., and Xu, H. 2011. "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly* (35:4), pp. 989-1015.

Smith, H. J., Milberg, S. J., and Burke, S. J. 1996. "Information Privacy: Measuring Individuals' Concerns About Organizational Practices," *MIS Quarterly* (20:2), pp. 167-196.

Solove, D. J. 2006. "A Taxonomy of Privacy," *University of Pennyslvania Law Reveiw* (154:3), pp. 477-564.

US Censor News. 2014. "Quarterly Retail Ecommerce Sales," (*http://www2.census.gov/retail/releases/historical/ecomm/14q3.pdf*. retrieved February 16th, 2014).

Van Slyke, C., Shim, J. T., Johnson, R., and Jiang, J. 2006. "Concern for Information Privacy and Online Consumer Purchasing," *Journal of the Association for Information Systems* (7:6), pp. 415-444.

Westin, A. F. 1991. "Domestic and International Data Protection Issues," *How the American Public Vies Consumer Privacy Issues in the Early 90s-and Why*, testimony before the Subcommitte on Government Information and Agriculture, Committee on Government Relations, U.S. House of Representatives, Washington, D.C., U.S. Government Printing Office, pp. 54-68.

Westin, A. F. 1967. *Privacy and Freedom,* New York: Atheneum.

Xu, H., Teo, H. –H., Tan, B. C. Y., and Agarwal, R. 2010. "The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services," *Journal of Management Information Systems* (26:3), pp. 135-173.

Appendix

Hypotheses	
H1a.	A high level of distrust is associated with a high level of privacy concern
H1b.	Distrust is associated with brain activity in the amygdala and insular cortex
H2a.	A high level of uncertainty is associated with a high level of privacy concern
H2b.	Uncertainty is associated with brain activity in the orbitofrontal cortex and the inferior parietal cortices
H3.	A high level of uncertainty is associated with a high level of privacy risk
H4a.	A high level of privacy risk is associated with a high level of privacy concern
H4b.	Privacy risk is associated with high levels of brain activity in the insular cortex when considering loss
H4c.	A high level of privacy risk is associated with brain activity in the nucleus accumbens when considering risk aversion
H5.	A high level of privacy risk is associated with a low level of personal information disclosure
H6.	A high level of privacy risk is associated with a high level of trust
H7.	A high level of privacy concern in associated with a low level of personal information disclosure
H8a.	A high level of trust is associated with a high level of personal information disclosure
H8b.	Trust is associated with brain activity in the caudate nucleus and putamen
H9a.	A high level of personal interest is associated with a high level of personal information disclosure
H9b.	Personal interest is associated with high brain activation in the ventromedial prefrontal cortex, and low activation in the dorsolateral prefrontal cortex