2017

The Role of Cognitive Disposition in Re-examining the Privacy Paradox: A Neuroscience Study

Zareef Mohammed
Nova Southeastern University, zm58@nova.edu

The Role of Cognitive Disposition in Re-examining the Privacy Paradox: A Neuroscience Study

by

Zareef Mohammed

A dissertation submitted in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

in

Information Systems

College of Engineering and Computing

Nova Southeastern University

2017

We hereby certify that this dissertation, submitted by Zareef Mohammed, conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.

Gurvirender Tejay, Ph.D. Chairperson of Dissertation Committee	Date
Steven R. Terrell, Ph.D. Dissertation Committee Member	Date
Ling Wang, Ph.D. Dissertation Committee Member	Date

Approved:

Yong X. Tao, Ph.D., P.E., FASME Dean, College of Engineering and Computing	Date

College of Engineering and Computing
Nova Southeastern University

2017

An Abstract of a Dissertation Submitted to Nova Southeastern University in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy in Information Systems

The Role of Cognitive Disposition in Re-examining the Privacy Paradox: A Neuroscience Study

by
Zareef A. Mohammed

The privacy paradox is a phenomenon whereby individuals continue to disclose their personal information, contrary to their claim of concerns for the privacy of their personal information. This study investigated the privacy paradox to better understand individuals' decisions to disclose or withhold their personal information. The study argued that individuals' decisions are based on a cognitive disposition, which involves both rational and emotional mental processes. While the extended privacy calculus model was used as the theoretical basis for the study, the findings of cognitive neuroscience was applied to it to address its limitation in assuming individuals are purely rational decision-makers. Three within-subjects experiments were conducted whereby each subject participated in all three experiments as if it were one. Experiment 1 captured the neural correlates of mental processes involved in privacy-related decisions, while experiment 2 and 3 were factorial-design experiments used for testing the relationship of neural correlates in predicting privacy concerns and personal information disclosure. The findings of this study indicated that at least one neural correlate of every mental process involved in privacy-related decisions significantly influenced personal information disclosure, except for uncertainty. However, there were no significant relationships between mental processes and privacy concerns, except Brodmann's Area 13, a neural correlate of distrust. This relationship, however, had a positive relationship with privacy concerns, opposite to what was hypothesized. Furthermore, interaction effects indicated that individuals put more emphasis on negative perceptions in privacy-related situations. This study contributed to the information privacy field by supporting the argument that individuals' privacy-related decisions are both rational and emotional. Specifically, the privacy paradox cannot be explained through solely rational cost-benefit analysis or through an examination of individuals' emotions alone.

Acknowledgements

Without any doubt, I say that this dissertation, and thereby my journey through this PhD. would not have been completed without the support of my father, Dr. Majeed Mohammed. He has supported me financially and mentally, and sacrificed so much for me, that I dedicate whatever success I have attained to him. Additionally, I thank my family; my beloved mother and sisters, my brother-in-law, and my two adorable nieces. They have each contributed to the completion of this dissertation, each supported me, whether they are aware of it or not, and without them all, I would not have had the motivation to endure this journey.

My eternal gratitude goes to my advisor, Dr. Gurvirender P. Tejay. I cannot thank him enough for all that he is done, nor could I ask for a better advisor, ever! He pushed me to evolve as a researcher, challenged me when I needed it, and supported me whenever I faced hurdles during this PhD., as well as through life. I do not know how I can ever repay Dr. Tejay, as he is the greatest mentor I have ever had in my life. I would like to thank my committee members, Dr. Ling Wang and Dr. Steven Terrell, who have provided excellent feedback and support in this dissertation. I learnt a lot from Dr. Wang with regards to quantitative research methods, that I am grateful she was on my committee and provided valuable feedback during my dissertation. I still remember the first time I met Dr. Terrell, he offered to help me whenever I needed it, and by extension became a valuable member of the committee.

Finally, my acknowledgements would not be complete without mention of my colleagues, Dr. Tejay's students. We would gather in the evenings of cluster sessions, and have discussions on our research goals, exploring the weaknesses in each other's studies, just so that we can strengthen them. My thanks to all of you, some of whom I met regularly, some who were before my time and I met on occasion, however, your insights were much appreciated. Special thanks go to the group of colleagues who I spent the most time with during this PhD.: Patrick Offor, my friend, my brother, and my rival; Darrell Eilts; Osborne Obeng; Fernando Lopez; and of course, my brothers, Abdul Rahim Charif and Joseph Squillace. Abdul, Joe and I would meet with Dr. Tejay very regularly; at the very least, on a weekly basis. These meetings were necessary to us, as they helped us grow as researchers, and friends. I would also like to thank Dr. James Lewis, who came for my dissertation defense. That support was greatly appreciated. And to my "Trini" friend, Kim, it was a pleasure meeting you every cluster. However, I do not believe the completion of this dissertation ends anything. I believe the bonds my colleagues and I built during the duration of my PhD. was only the prologue to a longer journey in research and life.

As I end these acknowledgements, I feel as if my words are too empty to express the emotions I feel to all who supported me. It is for this that I hope that my actions in the future can express even a fraction of the gratitude I feel.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

1.1. Introduction

The introduction and evolution of information and communication technologies (ICTs) have delivered a plethora of benefits such as the increase of communication and innovative means of marketing products and services. The impact of information systems (IS) on everyday human life is considered a utility similar to that of water, electricity, gas and telephone (Buyya, Yeo, Venugopal, Broberg, & Brandic, 2008). Yet, despite the advantages provided by information systems, there are disadvantages that are potentially dangerous to the individuals that use them. For instance, information privacy is a major concern (Mason, 1986), whereby personal information could often be compromised and used negatively.

Through the use of information systems, individuals can leverage their personal information to attain something else of value. This can be observed through the example of ecommerce websites, which allows individuals to purchase products and services, but require individuals to disclose their personal information. In turn, organizations could use the personal information of their customers to profile them, whereby organizations could develop stronger rapport with their customers, thereby growing their business (Awad & Krishnan, 2006; Culnan & Armstrong, 1999). Yet, the trade of personal information is considered a “double-edged sword” whereby personal information could be both an asset to an individual and a risk (Malhotra, Kim, & Agarwal, 2004). Organizations could use the personal information they have collected about an individual unethically such as selling it to third parties (Culnan, 1993; Smith, Milberg, & Burke, 1996), as well as reuse the collected personal information legally, but in ways that are unsanctioned by the owners (i.e. clients/customers) of the personal information (Culnan & Williams, 2009). Due to these risks, consumer reports and surveys have often revealed that individuals have great concerns over the privacy of their personal information (Dinev & Hart, 2006; Madden, Fox, Smith, & Vital, 2007; Smith, Dinev, & Xu, 2011).

Privacy concerns increase individuals' reluctance to disclose personal information, and subsequently impedes the use of information systems, such as ecommerce or ehealth, which requires individuals to disclose their personal information (Angst & Agarwal, 2009; Dinev & Hart, 2006; Li, Sarathy, & Xu, 2011). This is reflected by United States (US) trade data where ecommerce sales accounted for only 7% of total retail sales, indicating that the adoption and growth of ecommerce have not reached its full potential (US Census Bureau News, 2015). Similarly, while governments have invested in ehealth for safer and more efficient healthcare systems (Angst & Agarwal, 2009), patients are concerned about their personal medical records (Bishop, Holmes, and Kelley, 2005). It is therefore necessary to understand how both individuals and organizations could capitalize on the benefits provided by information systems, without compromise to personal information.

Researchers identified the privacy paradox as a fundamental issue whereby a conflict of interest exist between individuals' stated intentions and actual behavior regarding privacy related decisions (Norberg, Horne, & Horne, 2007). The privacy paradox occurs when individuals claim privacy concerns, yet continue to disclose their personal information (Dinev & Hart, 2006; Smith et al., 2011). By understanding the privacy paradox, organizations could potentially grow their businesses through the benefits of information systems. Similarly, the benefits through the use of information systems should be maximized by individuals, while reducing the vulnerability to information privacy. The privacy paradox becomes a key issue in understanding why individuals are willing to disclose their personal information, and if their decisions are reflective of good judgment regarding their information privacy.

1.2. Research Problem and Argument

This study investigated the privacy paradox to better understand individuals' decisions to withhold or disclose their personal information. Researchers have studied the privacy paradox in the context of ecommerce (Acquisti, 2004; Dinev & Hart, 2006; Norberg et al., 2007), personalization (Awad & Krishnan, 2006; Culnan & Armstrong, 1999), ehealth (Anderson & Agarwal, 2011; Angst & Agarwal, 2009), location based services (Xu, Teo, Tan, & Agarwal, 2012), and web 2.0 technologies (Dinev, Smith, & Xu, 2009). Yet, despite the impact the context may have on influencing individuals' decisions to disclose personal information, privacy concerns are consistent in negatively affecting the disclosure of personal information (Anderson & Agarwal, 2011; Awad & Krishnan, 2006; Dinev and Hart, 2006; Xu et al., 2010). Therefore, despite the difference in value of the medium in influencing individuals' disclosure of personal information (Awad & Krishnan, 2006), it is necessary to understand the role of individuals' perceptions in shaping their privacy related decisions.

In seeking to understand the privacy paradox, researchers have often assumed individuals are rational decision-makers (Acquisti, 2004; Acquisti & Grossklags, 2005), where multiple factors may subvert the negative effect privacy concerns have over personal information disclosure (Smith et al., 2011). Trust has often been found to be a plausible explanation as to why individuals would disclose their personal information despite claims of concerns (Belanger, Hiller, & Smith, 2002; Dinev & Hart, 2006; Pavlou, Liang, & Xue, 2007; Van Slyke, Shim, Johnson, & Jiang, 2006). Essentially, an individual's propensity to trust an entity to properly handle the personal information he/she is required to disclose would override their privacy concerns. Yet, trust and privacy concerns are not the only factors to be considered since privacy risk has also been observed to be a salient factor in the privacy paradox (Dinev & Hart, 2006; Malhotra et al., 2004; Norberg et al., 2007). While privacy concerns and privacy risks are closely related, Dinev and Hart (2006) considered them to be distinct. Furthermore, risk may not be one dimensional as often assumed, but may involve both the assessment of loss as well as the probability of avoiding a risky action (Peter & Tarpey, 1975; Smith et al., 2011).

The conflicting nature of the privacy paradox has led to the development of the privacy calculus, which assumes individuals perform a cost-benefit analysis when they decide to disclose their personal information (Culnan & Bies, 2003; Dinev & Hart, 2004; 2006; Smith et al., 2011). The privacy calculus assumes that individuals would be more likely to disclose their personal information if the benefits outweigh the costs (Laufer & Wolfe, 1977). Based on this cost-benefit assumption, Dinev and Hart (2006) argued that individuals' decisions to disclose their personal information consists of contrary but salient factors, which included trust, privacy concerns, and privacy risks. Additionally, Dinev and Hart (2006) considered personal interest as a factor that could override the negative impacts of privacy risk and privacy concerns. Similarly, Van Slyke et al. (2006) found similar factors of trust, privacy risk, and privacy concerns as key indicators to individuals' decisions to disclose personal information. Yet, the cost-benefit assumption is limited by the reality that humans are not purely rational decision-makers (Acquisti & Grossklags, 2005).

Acquisti (2004) explained that several psychological deviations limit rationality from individuals. Acquisti (2004) explained that people are subject to bounded rationality, whereby they do not have knowledge of all the parameters governing a privacy-related decision, and even if they did, they would not be able to accurately process all of these parameters. Moreover, cognitive biases such as hyperbolic discounting, where individuals prefer short-term gratifications, affect rationality in privacy-related decisions (Acquisti, 2004). Evidently, research from the cognitive neuroscience field has identified a number of brain areas that are correlated with mental processes such as perceptions of risk and trust (Dimoka, Pavlou, & Davis, 2007; 2011). Furthermore, these brain activations occur in both the prefrontal cortex (rational decisions) and limbic system, which are responsible for emotional responses (Dimoka et al., 2007). The prefrontal cortex and limbic system interacts with one another extensively, indicating that rationality and emotions are often intertwined (Phelps, 2006). Essentially, no decision is purely rational or purely emotional. Based on the findings of cognitive neuroscience, it can be assumed that both rationality and emotions play a role in individuals' decisions to disclose their personal information. As such, this research argued that individuals' disclose their personal information based on their cognitive disposition, which includes rational and emotional mental processes.

1.3. Importance of Research Problem

Privacy is a concept that has been present in philosophical debates and social science research, such as psychology, sociology, political science, as well as other fields (Smith et al., 2011). The emergence of ICTs has highlighted the importance of a specific subset of privacy, i.e. information privacy, as a major concern in the digital age (Mason, 1986). Specifically, the evolution of ICTs allows for increased surveillance, computation, storage and retrieval of individuals' personal information (Mason, 1986). Organizations gain valuable strategies for continued development through data mining techniques using individuals' personal information (Li & Sarker, 2006; Mason, 1986). Additionally, the growth of the internet provides convenient business transactions for individuals, as well as increased communications. Moreover, individuals use the internet and other innovative web applications to become content providers (Hong & Thong, 2013). Essentially, this leaves individuals vulnerable to privacy-related threats (Culnan & Williams, 2009; Hong & Thong, 2013). While individuals continue to voice concerns for the privacy of their personal information (Dinev & Hart, 2006; Smith et al., 2011), specific laws and regulations are enacted by governments in hope of protecting individuals' personal information (Culnan & Williams, 2009; Greenaway, Chan, & Crossler 2015). Yet, many such regulations are ineffective in adequately protecting individuals' personal information (Culnan & Willaims, 2009); while individuals' behavior deviate from their voiced privacy concerns in their increased disclosure of personal information using ICTs (Smith et al., 2011).

Individuals' contradictory behavior of stating their concerns for the privacy of their personal information, yet continuing to disclose their personal information for certain benefits, termed the privacy paradox, has been extensively studied by multiple researchers (Acquisti, 2004; Acquisti & Grossklags, 2005; Awad & Krishnan, 2006; Belanger & Crossler, 2011; Dinev & Hart, 2006, Norberg et al., 2007; Smith et al., 2011). It was found that individuals' privacy beliefs and their associated privacy-related behavior could be classified into three categories: privacy fundamentalists, privacy pragmatists, and privacy unconcerned (Harris Interactive & Westin, 2002). While privacy fundamentalists were more skeptical of disclosing their personal information, and fought for privacy regulations, privacy pragmatists were more likely to estimate the risks and costs in disclosing their personal information (Angst & Agarwal, 2009; Awad & Krishnan, 2006; Harris Interactive & Westin, 2002). Individuals who were identified as privacy unconcerned, however, would readily disclose their personal information, without much concern or emphasis to the concept of information privacy (Angst & Agarwal, 2009).

The beliefs of individuals with regards to information privacy, and subsequently personal information disclosure, has often been investigated by researchers (Dinev & Hart, 2006; Norberg et al., 2007; Pavlou et al., 2007; Van Slyke et al., 2006), while often connecting these beliefs to the three privacy categories of individuals (Awad & Krishnan, 2006; Angst & Agarwal, 2009). A number of contradictory beliefs (negative and positive factors) emerge from extant literature that is found to directly influence individuals to disclose or withhold their personal information (Dinev & Hart, 2006). Among these beliefs are privacy concerns, privacy risk, institutional trust (i.e. the propensity to trust), and uncertainty (Awad & Krishnan, 2006; Belanger et al., 2002; Dinev & Hart, 2006; Malhotra et al., 2004; Norberg et al., 2007; Pavlou et al., 2007; Van Slyke et al., 2006).

Additionally, studies have indicated that other factors such as culture, regulations, organizations' privacy practices (such as privacy seals, privacy statements, and organizations' transparency of the use of collected personal information), and methods of persuasion were related to privacy beliefs (Awad & Krishnan, 2006; Angst & Agarwal, 2009; Dinev, Bellotto, Hart, Russo, Serra, & Collautti, 2006; Li et al., 2006; LaRose & Rifon, 2006; Milberg, Smith, & Burke, 2000).

While an individuals' privacy beliefs, along with other related antecedents may inform privacy-related behavior, some researchers point out that privacy-related decision-making may be limited by individuals' cognitive capabilities (Acquisti & Grossklags, 2005). As argued by Acquisti (2004), multiple cognitive biases, such as cognitive overload (inability to cognitively process all parameters of a given situation), may affect individuals' privacy-related decisions. Specifically, individuals' decisions are not purely rational, which may often result in outcomes that seem contrary to their beliefs. Similarly, Sim, Liginlal, and Khansa (2012) advocated that individuals' decisions with regards to the privacy of their personal information may be subjected to situational awareness (an individual's ability to handle a situation in space and time with their restricted cognitive abilities).

While understanding the intrinsic beliefs, as well as the extrinsic factors that may influence such beliefs could provide an explanation to the privacy paradox, a better understanding of individuals' privacy-related decision-making could be elicited by examining individuals' perceptions in privacy situations. Specifically, while intrinsic and extrinsic factors may be antecedents of privacy concerns and privacy-related decisions, the momentary cognitive and affective state before an individual makes a decision with regards to information privacy should be considered. Current literature has investigated individuals' privacy beliefs (Dinev & Hart, 2006; Van Slyke et al., 2006), the factors which may affect these beliefs (Angst & Agarwal, 2009; Li et al., 2011), as well as the cognitive limits of individuals in privacy-related situations (Acquisti, 2004; Anderson & Agarwal, 2009). However, a gap in the literature exists in observing how individuals' perceptions are formed and relate to one another when they are in a situation requiring them to disclose their personal information. Findings in cognitive neuroscience has indicated that human behavior is often influenced by the processing of some external stimuli, before conscious thought (Dimoka, 2010; Dimoka et al., 2007; 2011; Sur & Sinha, 2009; Vance, Eargle, Anderson, & Kirwan, 2014). Essentially, while long held beliefs and other intrinsic and extrinsic factors may play a role in privacy-related decisions, the state of an individual produced by a privacy-related decision (such as whether to disclose personal information to an online seller or for entry into an electronic health system) may be more effective in determining privacy-related decisions. Thus, this study argued that individuals disclose their personal information based on their cognitive disposition, which is both rational and emotional. Since rationality and emotions are often interconnected (Phelps, 2006), this study contributes to the field of information privacy by providing a better explanation of the privacy paradox by addressing the current gap in the literature.

With the proliferation of data produced at an exponential rate, information privacy has become an issue that affects both society and organizations. Organizations continue to invest in and promote the use of various ICTs for data mining purposes to remain competitive (Awad & Krishnan, 2006; Culnan & Armstrong, 1999). So as to not waste investments and resources into innovative ICTs, organizations could enact strategies based on knowledge derived from understanding the privacy paradox, to motivate individuals to disclose their personal information. However, the rise of big data and emergence of new technologies, such as virtual reality and the internet-of-things (IoT), individuals' information privacy become further threatened. Understanding the privacy paradox could enable individuals, privacy-activists, and government to increase awareness of information privacy issues and develop strategies for individuals to further protect their personal information, such as the development and use of privacy enhancing technologies, as well as laws and regulations that are designed more proactive as opposed to reactive (Culnan & Williams, 2009; DeGeorge, 2006)

1.4. Definition of Key Terms

Personal Information – also referred to as 'personally identifiable information', can be defined as information that can specifically identify someone, such as name, address, social security number; as well as financial information such as credit card numbers (Caudill & Murphy, 2000; Dinev & Hart, 2006). Additionally, personal information may comprise of aggregated non-identifying information used for market analysis, or for profiling when used in combination with identifiable information (Caudill & Murphy, 2000; FTC, 1998). Personal information may often be defined based on context, such financial information in ecommerce, electronic health records in ehealth, digital content hosted by content providers, digital surveillance in the workplace and in individuals' homes (Hong & Thong, 2013; Smith et al., 2011). Essentially, personal information is broad enough to include a variety of situations that currently exist and evolve throughout space and time (Hong & Thong, 2013; Smith et al., 2011).

Privacy – General privacy has been applied to almost all fields of the social sciences, yet does not have a clear definition consistent across all disciplines (Smith et al., 2011). Warren and Brandeis (1890) defined privacy as the human right to be left alone. According to Smith et al. (2011), privacy as a human right was the first definition of general privacy, whereby privacy is considered integral to a society's moral value system. Due to the broadness of privacy, different disciplines assigned different meanings to it, such as the commodity view of privacy with regards to the field of economics (Smith et al., 2011). Specifically, researchers across disciplines may not be able to fully articulate what privacy means due to the outcomes of each context to which privacy is applied (Belanger & Crossler, 2011; Smith et al., 2011; Solove, 2006). However, privacy is an overarching concept which incorporates information privacy (Smith et al., 2011).

Information Privacy – Information privacy is a subset of the overall concept of general privacy because of the complex issues arising from the introduction and evolution of ICTs (Belanger and Crossler, 2011; Smith et al., 2011). There are many definitions for information privacy, whereby researchers have classified information privacy into two broad categories of value-based and cognate-based definitions (Smith et al., 2011). Value-based definitions regard information privacy as an objective societal value, whereas cognate-based definitions are related to individual's mind, perceptions and cognitions (Smith et al., 2011). For the purposes of this dissertation, Westin's (1967) definition of information privacy is adopted which refers to the control an individual has over the collection, use and dissemination of his/her personal information. A cognate-based definition of information privacy as a control is suited for this study as an individual's belief of the control he/she has over his/her personal information may drive his/her rational and emotional perceptions that influence his/her privacy-related decisions.

Privacy Paradox – The privacy paradox refers to the inconsistency of individuals' decisions whereby they disclose their personal information despite claiming concerns for the privacy of their personal information (Dinev & Hart, 2006; Norberg et al., 2007). Researchers have often used privacy concerns as a measure of an individual's perception of privacy (Smith et al., 2011). Studies have thus found privacy concerns to inhibit individuals from disclosing their personal information (Awad & Krishnan, 2006; Dinev & Hart, 2004; 2006; Smith et al., 2011). Yet, despite these privacy concerns, there is some growth in the use of ICTs that require individuals to disclose their personal information. As such, the privacy paradox exists when individuals' claim that information privacy is important, but their behavior is contradictory to their claims.

Cognitive Disposition – An individual's cognitive disposition refers to the rational and emotional mental processes that govern the decisions the individual makes (Dimoka et al., 2007; 2011). An individual's mental processes correlate with specific areas of the brain. In the brain, the prefrontal cortex is responsible for processing rationality, whereas the limbic system processes emotions (Dimoka et al., 2007). However, both the prefrontal cortex and limbic system interact with one another, suggesting that rationality and emotional processing are intertwined (Dimoka et al., 2007; 2011; Phelps, 2006). Essentially, an individual does not make a decision that is based solely on rationality, nor purely emotions, but rather an individuals' decisions consist of both rational and emotional mental processes.

1.5. Summary

The privacy paradox is a phenomenon whereby individuals claim concerns for the privacy of their personal information, but act contrarily by disclosing their personal information to organizations and websites in return for small benefits. The information privacy field studies this phenomenon so that both organizations and individuals may obtain the maximum benefit of using ICTs, but without the compromise to individuals' personal information. The privacy paradox has often been studied as a phenomenon that occurs due to some rational thought process or calculation by individuals. However, individuals are not purely rational, and may be subjected to emotional impulses. Essentially, studying the privacy paradox from individuals' cognitive disposition (i.e. both rational and emotional mental processes) should enhance the current understanding of individuals' privacy-related decisions, which is the objective of this study.

Chapter 2

Literature Review

2.1. Introduction

This chapter reviews literature which is related to the topic of this dissertation. The findings and contributions of prior literature need to be understood so that gaps within the literature could be identified, and arguments could be clearly articulated. This literature review is separated into three main sections, which begins with discussing the concept of information privacy followed by how information privacy has often been studied by researchers using privacy concerns as a measure of information privacy. Literature pertaining to the privacy paradox is then reviewed to complete the literature review of this study.

2.2. Information Privacy

Privacy is an issue within the disciplines of philosophy and other social sciences that is at least over a century old (Belanger & Crossler, 2011; Smith et al., 2011). However, the introduction of ICTs within the everyday lives of individuals has brought an invested interest in the implications of the privacy of individuals' personal information. Specifically, information privacy is a subset of general privacy that has incited numerous studies by researchers (Belanger & Crossler, 2011; Pavlou, 2011; Smith et al., 2011). However, while information privacy is of great relevance to society, it is still a fragmented concept which has not yet been fully defined (Solove, 2006).

The most inclusive definition of information privacy explains that it is the control an individual has over the collection and use of his/her personal information (Smith et al., 1996; Westin, 1967). Yet, personal information is a resource from which individuals and organizations could gain multiple benefits. As such, individuals and organizations continue to exchange personal information for these benefits despite the presence of risks. Researchers have attempted to understand the role of information privacy in society, as well as how it impacts the adoption of ICTs (Belanger & Crossler, 2011; Smith et al., 2011).

Prior studies have found that the concept of information privacy could be categorized as either value-based or cognate-based (Smith et al., 2011). Within the value-based category, information privacy is regarded as either a right or a commodity, whereby individuals' personal information has an actual value within the framework of society (Smith et al., 2011). However, the cognate-based approach to information privacy interprets privacy as an individuals' subjective value assessment of his/her personal information. The cognate-based definitions of information privacy further categorize information privacy as a state or a control (Smith et al., 2011). Essentially, the value-based category of information privacy differs from the cognate-based category since it assumes that privacy is an assigned value of the society, whereas the cognate-based category is related to individuals' mind, perceptions and cognitions (Smith et al., 2011).

2.2.1. Privacy Defined as a Value

When privacy is regarded as a value, it is further categorized as either a right, or a commodity. Privacy defined as a human right to be left alone is deemed as a necessity in maintaining a society's moral value system (Clarke, 1999; Skinner, Han, & Chang, 2006; Smith et al., 2011). Explaining information privacy as a right stem from the debates of general privacy as a human right which is highly discussed in the legal and political fields (Smith et al., 2011). Stemming from an article by Warren and Brandeis (1890), which defined general privacy as the "right to be left alone", influenced US law in recognizing privacy as a salient issue to society. This led to numerous legal cases which advocated privacy as each individual's right to be left alone and covered a number of themes such as privacy and the press, privacy and law enforcement, privacy and voyeurism, and privacy in the workplace (Alderman & Kennedy, 1997; Smith et al., 2011).

The US established the “Privacy Act of 1974” based on the notion that privacy is a human right, whereby individuals could still be protected from unwarranted invasion of their privacy by government agencies (The Privacy Act of 1974). The recognition of privacy as a societal issue within the information age led to the development of the federal trade commission (FTC) fair information practices (FIPs) which described four main dimensions of notice, access, choice and security within the electronic marketplace for the protection of individuals’ personal information (Liu & Arnett, 2002). While the US FIPs allowed for organizations to regulate themselves by establishing the FIPs within their business processes, other regulations and laws were established for different industry sectors to better protect the personal information organizations collected (Culnan & Williams, 2009). For example, the Health Insurance Portability and Accountability Act (HIPAA) is one such regulation to which healthcare organizations are required to adhere (Culnan & Williams, 2009).

Yet, the debate about privacy as a human right as integral to the structure of the society's moral system suffers from the limitation that privacy does not hold the same value in the varied cultures and governmental bodies throughout the world (Smith et al., 2011). In fact, the European Union (EU) differs from the US in the view of privacy, where they focus on the implementation and enforcement of safeguards for organizations to fairly manage individuals' personal information (Rose, 2006). Also, despite the view that individuals' privacy is a human right, when examining consumer behavior, a privacy paradox was observed whereby individuals continue to trade their personal information for specific benefits (Smith et al., 2011). This lead to the shift in the definition that the value of privacy was more regarded as a commodity than a human right (Smith et al., 2011).

Researchers adopted the commodity-based definition of information privacy when they observed the apparent cost-benefit analysis individuals undergo when deciding to disclose or withhold their personal information. (Acquisti & Grossklags, 2005; Culnan & Armstrong, 1999; Dinev & Hart, 2006; Norberg et al., 2007). Essentially, the commodity-based definition holds that an individual's personal information is valuable, but he/she may be willing to trade his/her personal information for something else of equal value. Assigning an economic value to information privacy differentiates the definition of privacy as a commodity from privacy as a right (Smith et al., 2011). Specifically, while both definitions regard information privacy as an objective value in society, when privacy is defined as a commodity, it essentially means that the individual may lose ownership of his/her personal information. Conversely, privacy as a human right retains the notion that even if an individual were to disclose his/her personal information to some other person or organization, the individual's personal information would still be required to be protected and used only based on the individual's permission (Culnan & Williams, 2009; Solove, 2006; Smith et al., 2011).

2.2.2. Privacy Defined as Cognate-based

The cognate-based definitions of state and control assumes that privacy is decided by the individual him/herself. Schoeman (1984) explained that general privacy is a state of "limited access to a person" (p. 3), whereby Westin (1967) viewed privacy as consistent of an individual's anonymity, solitude, reserve and intimacy. Essentially, the paradigm of privacy as a state is defined by an individual's choice to seek privacy or disclose his/her personal information, which is influenced by situations which includes self-ego, environmental, and interpersonal factors (Laufer & Wolfe, 1977). With regards to information privacy, a state-based definition posits that individuals’ subjective cognitions of the situations in which they are asked to disclose their personal information would direct their decisions.

A widely accepted definition of privacy within the field of information systems, as well as other fields such as philosophy, social and political sciences, psychology and marketing assumes that privacy is based on the level of control an individual has over his/her personal information (Smith et al., 2011). Specifically, as long as an individual assumes that he/she can control the use of his/her personal information, and minimize the risks posed by disclosing it, he/she would be willing to provide his/her personal information to other entities. The control-based definition of general privacy is rooted in the definition by Westin (1967), as well as that of Altman (1975) as "the selective control of access to the self" (p. 24). Margulis (1977) captured the essence of the control-based definition of privacy by explaining "privacy, as a whole or in part, represents the control of transactions between person(s) and other(s), the ultimate aim of which is to enhance autonomy and/or to minimize vulnerability" (p. 10). Yet, there exists another debate between researchers by what is meant by “privacy is a control” (Smith et al., 2011). Smith et al. (2011) explained that some researchers considered privacy in and of itself as a control, whereas others assumed that control is a key factor of privacy. As explained by Laufer and Wolfe (1977), an individual may assert some level of control over his/her personal information, however that does not equate to privacy. Control, however, may be a key factor in achieving privacy (Laufer & Wolfe, 1977; Smith et al., 2011).

2.2.3. Privacy within the Information Systems Field

With regards to the information systems field, researchers have conducted a number of studies by categorizing privacy in one of the four above mentioned definitions, so as to gain a better understanding of the concept (Smith et al., 2011). Adopting a definition to information privacy allows researchers to better understand how the concept of information privacy relates to other factors (Pavlou, 2011; Smith et al., 2011). Essentially, the only way to understand the role of information privacy in individuals' lives is by understanding its meaning and relationship with other factors that drive individuals' behavior towards specific tasks.

Similar to the fields of law and political sciences where privacy is often defined as a human right (Smith et al., 2011), a number of studies in the IS discipline have also adopted a right-based definition (Liu, Marchewka, Lu, & Yu, 2005; Malhotra et al., 2004). Yet, a review of empirical studies suggest that this view of privacy is limited in the IS field. Schwaig, Kane, and Storey (2006) found that less than four percent of the Fortune 500 companies' websites actually complied with all aspects of fair information practices. If privacy is a right, then individuals should be reluctant in disclosing their personal information to organizations that have ambiguous privacy practices. Yet, as Hsu (2006) found, individuals stated privacy concerns do not match their behavior in disclosing personal information. As such, a large number of studies in the IS field have adopted a control-based definition of information privacy assuming that individuals' perceptions of control over their personal information drive them towards decisions of information disclosure (Belanger & Crossler, 2011; Culnan & Bies, 2003; Dinev & Hart, 2004; Van Slyke et al. 2006). Alternatively, a growing number of studies adhere to the rational commodity trade-off of information privacy to specific benefits, since it logically explains the current paradox of individuals' personal information disclosure, yet high levels of privacy concerns (Acquisti, 2004; Dinev & Hart, 2006; Norberg et al., 2007).

Due to the multiple streams of research into information privacy, as well as the conflicting findings, the concept is still inconsistent and requires much study (Pavlou, 2011; Smith et al., 2011). Researchers have often used privacy concerns as a means of measuring information privacy, since information privacy is often regarded as complex and near impossible to measure by itself (Dinev et al., 2009; Smith et al., 2011). While Dinev et al. (2009) regarded privacy concerns as inadequate to fully understand information privacy, privacy concerns as a construct is a representation of the negative perceptions an individual has over the collection and use of his/her personal information he/she may be required to disclose to another person or organization.

2.3. Measuring Information Privacy Through Privacy Concerns

Privacy concerns have often been studied as a proxy for measuring the concept of information privacy, due to the complexity and immeasurable nature of information privacy itself (Dinev et al., 2009; Smith et al., 2011). Understandably, studies in the IS discipline seek to examine how information privacy affects the use of technologies, and as such, researchers have treated information privacy as a negative factor (Dinev et al., 2009). This is further justified based on the evidence presented from polls whereby individuals claim a high level of concern for the privacy of their personal information (Dinev & Hart, 2006; Madden et al., 2007; Smith et al., 2011). Similarly, numerous studies have found that privacy concerns inhibit individuals from disclosing their personal information (Dinev & Hart, 2006; Li et al., 2011; Pavlou et al., 2007; Van Slyke et al., 2006).

Smith et al. (1996) developed the concern for information privacy (CFIP) instrument which consisted of four dimensions to measure individuals' concerns over the information handling techniques of organizations. The CFIP consists of four dimensions of concerns individuals have over their personal information: collection, errors, secondary use, and improper access (Smith et al., 1996). Collection refers to the extensive collection and storage of the personal information of individuals, whereas secondary use pertains to the use of such personal information of individuals for purposes apart from that which was stated (Smith et al., 1996). This would include selling the personal information to third party organizations. Individuals are also concerned about the access others may have to their personal information, despite the lack of proper authorization. Finally, errors refer to the concern individuals may have over the deliberate and accidental errors to their personal information, and the lack of safeguards towards such cases (Smith et al., 1996).

While the CFIP instrument was developed to capture individuals' privacy concerns, and measure these concerns with regards to other factors in relation to individuals' adoption of ICTs (such as ecommerce, or ehealth), Stewart and Segars (2002) found that CFIP may be better represented as a higher-order factor structure rather than a set of first-order factors. Essentially, these findings indicated that individuals are concerned with all the dimensions of CFIP rather than one dimension (Stewart & Segars, 2002). As such, modeling the CFIP as a higher-order construct would allow for more accurate findings when measured with regards to other factors, which, may drive individuals to disclose or withhold their personal information (Stewart & Segars, 2002). However, Malhotra et al. (2004) explained that there were limitations to CFIP which did not account for the overall privacy concerns of individuals in situations where they are required to disclose their personal information.

Malhotra et al. (2004) developed the Internet Users' Information Privacy Concerns (IUIPC) instrument because of limitations of previous instruments such as the global information privacy concern (GIPC) and CFIP. Malhotra et al. (2004) explained that GIPC suffered from the lack of dimensionality in explaining individuals' privacy concerns, and CFIP was not an absolute scale. The change of the marketing environment because of the internet could impact the dimensions of privacy concerns individuals may have (Malhotra et al., 2004). As such, the IUIPC accounted for these limitations by developing a better scale for measuring and studying individuals' privacy concerns. Specifically, while CFIP is focused on individuals’ perceptions of how organizations handle collected personal information, IUIPC concentrated on the perceptions of fairness individuals may have when deciding to disclose their personal information (Malhotra et al., 2004). Therefore, the IUIPC essentially consists of individuals' perceptions of the collection of their personal information, the control they have over it, and also their level of awareness of privacy practices (Malhotra et al., 2004). However, despite the advantages of IUIPC over CFIP, researchers have often chosen to use the CFIP instrument when measuring privacy concerns (Rose, 2006; Van Slyke et al., 2006).

While researchers have often extensively used privacy concerns as a measure of information privacy (Dinev & Hart, 2006; Pavlou et al., 2007; Van Slyke et al., 2006), privacy concerns may be lacking to truly represent information privacy (Dinev et al., 2009). Essentially, privacy concerns may not represent individuals' overall perception of information privacy since a person's privacy may not be violated despite his/her high levels of privacy concerns (Dinev et al., 2009). Similarly, privacy concerns are negative, and therefore, contradicts the value of information privacy to any individual or society (Dinev et al., 2009). Essentially, the overall concept of information privacy may be a result of the relationship between factors such as privacy awareness, privacy beliefs, and privacy attitudes. Dinev et al. (2009) found that individuals' privacy attitudes were influenced by privacy beliefs which were preceded by privacy values. Similarly, Belanger and Crossler (2011) indicated that individuals' privacy attitudes differed from their privacy concerns. Therefore, while prior literature has indicated the saliency of privacy concerns with regards to information privacy, there are other measurable factors of information privacy that might provide a better understanding of the concept.

2.4. Privacy Paradox

The phenomenon of the privacy paradox involves the contradictory behavior of individuals whereby they express concerns for the privacy of their personal information, yet continue to disclose personal information to organizations (Dinev & Hart, 2006; Li et al., 2011; Norberg et al., 2007; Smith et al., 2011). It is expected that individuals would abstain from information disclosure since they express high concerns over the privacy of their information, yet anecdotal and empirical evidence suggest otherwise, thereby indicating that while privacy is an important issue to individuals, there are other factors which drive behavior beyond privacy (Dinev & Hart, 2006; Smith et al., 2011). The commodity-based definition of information privacy was based on the existence of the privacy paradox (Smith et al., 2011). Essentially, it is reasonable to assume that logically privacy is only one asset that could be traded for an equal or better asset.

Since information technologies are becoming a utility of modern society (Buyya et al., 2008), organizations and governments seek to influence individuals to disclose their personal information. From the organizational perspective, individuals' personal information could be used to increase rapport between the organization and their clients, thus contributing to organizational growth (Awad & Krishnan, 2006; Culnan & Armstrong, 1999). Similarly, from the individual and societal perspective, there are multiple benefits that could be gained from using innovative information technologies (Angst & Agarwal, 2009). It is only by understanding the privacy paradox, organizations, government, and society could maximize the benefits of information exchange and minimize the costs.

Research within the privacy paradox has been centered on various ICTs. Often, researchers would examine the privacy paradox with regards to online transactions (Acquisti, 2004; Dinev & Hart, 2006; Norberg et al., 2007). Findings have indicated that individuals' privacy concerns are an impediment to ecommerce transactions (Dinev & Hart, 2006; Li et al., 2011), yet individuals' online purchasing behavior outweigh their stated intentions (Norberg et al., 2007). Through the use of ICTs, organizations are able to gather a great deal of information on individuals' online shopping behavior and browsing habits. Furthermore, the collection of individuals' personal information could be used for online profiling. While online profiling could be used for both the benefits of organizations and individuals, it can incur heavy privacy concerns (Awad & Krishnan, 2006; Culnan & Armstrong, 1999; Sutanto, Palme, Tan, & Phang, 2013). Moreover, when the sensitivity of information is increased, there exists reluctance to personal information disclosure, such as in the case of medical information (Anderson & Agarwal, 2011; Angst & Agarwal, 2009; Bansal, Zahedi, & Gefen, 2010; Hsu, 2006). In essence, despite the context, privacy concerns have been found to have a negative effect in the disclosure of personal information (Dinev & Hart, 2006; Pavlou et al., 2007; Van Slyke et al., 2006).

The inconsistency posed by the privacy paradox has driven researchers to seek an understanding as to why individuals would provide their personal information despite their stated privacy concerns (Acquisti, 2004; Awad & Krishnan, 2006; Dinev & Hart, 2006; Norberg et al., 2007; Pavlou et al., 2007). Studies have indicated that as long as individuals retain a level of control of their personal information, they will be willing to disclose their personal information online (Awad & Krishnan, 2006; Culnan, 1993; 2000;

Culnan & Bies, 2003; Dinev & Hart, 2004). Culnan (1993) found that individuals with a positive attitude towards secondary information use were different from those with negative attitudes because of the level of control they had over their personal information.

Awad and Krishnan (2006) found that the importance of information transparency, which was defined as the "features that give consumers access to the information a firm has collected about them, and how that information is going to be used" (p. 14), influenced individuals to disclose their personal information. Similarly, when individuals perceived fairness in the handling of their personal information and subsequently felt they had control over their personal information, they were more likely to disclose their personal information (Culnan & Armstrong, 1999; Lin & Wu, 2008; Malhotra et al., 2004). However, Awad and Krishnan (2006) also found that between personalized services and personalized advertisement, individuals were more willing to participate in the former since it was more valuable, which essentially indicated that there was some perception of equivalent trade present. Thus, further investigations of the privacy paradox were carried out by researchers to elicit a more thorough understanding of individuals' privacy-related behaviors (Dinev & Hart, 2007; Kehr, Wentzel, & Kowatsch, 2014; Pavlou et al., 2007).

Privacy concerns contribute towards individuals' decisions to withhold personal information (Dinev & Hart, 2006; Van Slyke et al., 2007). However, as explained by Kehr et al. (2014), empirical evidence has shown that in the presence of other factors, privacy concerns are either insignificant, or more often, have small correlations with individuals' personal information disclosure, despite individuals' claims of privacy concerns. Essentially, privacy concerns may be subverted by other factors. Malhotra et al.

(2004) indicated that information sensitivity was a salient factor impacting individuals' behavioral intentions, risk beliefs and trust beliefs. Similarly, Dinev et al. (2009) found information sensitivity significantly impacted individual's perceived vulnerability, which in turn influenced individuals' privacy perception.

Studies have found that an important factor which was related to information privacy is that of trust (Belanger et al. 2002; Smith et al., 2011). Specifically, the trust built between organizations and individuals has been found to influence personal information disclosure (Malhotra et al., 2004; Smith et al., 2011), as well as mitigate privacy concerns (Belanger et al. 2002; Pavlou et al., 2007; Xu, Teo, & Tan, 2005). Yet, other studies have found that trust was negatively predicted by individuals' privacy concerns (Bansal, Zahedi, & Gefen, 2008; 2010; Chellappa, 2008; Malhotra et al., 2004). Dinev and Hart (2006) found trust to influence individuals' intentions to provide personal information, and subsequently transact online. Their findings were consistent with those of Van Slyke et al. (2006), who also found that if individuals' privacy concerns were higher, their trust would be lower. While individuals' privacy concerns significantly influenced their perceived uncertainty in ecommerce transactions, trust was found to be a mitigator of both information privacy and security concerns; and subsequently also mitigated the two other antecedents of perceived uncertainty: perceived information asymmetry and fears of seller opportunism (Pavlou et al., 2007). As such, the results of Pavlou et al. (2007) suggested that trust could influence individuals to provide their personal information, and transact online, to some degree.

Research has been done which identified the conditions under which individuals would trust an organization. With regards to building trust, Culnan and Armstrong (1999) found FIPs were significant in influencing individuals' disclosure of personal information. Their findings were consistent with that of Xu et al. (2012), whereby both industry self-regulation and government regulation of FIPs reduce the perceived risks of information disclosure. Similarly, individuals' trust in organizations increases with the use of privacy policies (Andrade, Kaltcheva, & Weitz, 2002; Hui, Teo, &Lee, 2007; Milne & Boza, 1999). The platform for privacy preferences project (p3p) compliance was found to increase trust which in turn influenced individuals to disclose their personal information (Xu et al., 2005). Likewise, Rifon, La Rose, and Choi (2005) found privacy seals positively influenced individuals trust perceptions, while Miyazaki and Krishnamurthy (2002) found privacy seals added to the positive effect privacy statements had on trust. However, contrary findings from Hui et al. (2007), as well as Moores (2005), both found privacy seals as insignificant in addressing privacy concerns. Specifically, while Hui et al. (2007) found privacy seals were less important than privacy statements, Moores (2005) found that individuals barely understand the role of privacy seals. Similarly, Norberg et al. (2007) questioned the overall influence of trust on individuals' behavior to disclose personal information when the results of their study found trust to be insignificant.

2.4.1. Privacy Calculus

Researchers within the field of information privacy have found that one of the most plausible explanations to individuals' behavior with regards to information privacy, is the privacy calculus (Dinev & Hart, 2006; Smith et al., 2011). While studies have found that individuals could be influenced to disclose their personal information; they could also choose to withhold their personal information under certain circumstances. As such, the privacy calculus delivered a logical explanation, in which individuals' privacy-related behavior was subject to a cost-benefit analysis (Smith et al., 2011). Specifically, the privacy calculus posited that there exists a rational calculus of salient but contrary factors in which individuals undergo when they are asked to disclose their personal information (Dinev & Hart, 2006). If individuals perceived a higher level of negative consequences in disclosing their personal information, they were less likely to do so; and similarly, a perception of greater benefits led to information disclosure (Dinev & Hart, 2006).

The origins of the privacy calculus lie in the studies that argued that individuals' behavior to disclose personal information was subject to a trade-off of benefits and costs, whereby economic or social benefits should outweigh the negative consequences (Culnan & Armstrong, 1999; Laufer & Wolfe, 1977; Posner, 1984; Stone & Stone, 1990). In their study, Dinev and Hart (2004) utilized the privacy calculus, which consisted of perceived vulnerability as the negative factor, and perceived ability to control as the positive factor. Their research model was rooted in the procedural justice framework which was found to motivate individuals to disclose their personal information (Culnan & Armstrong, 1999). As such, the perceived ability to control was posited to decrease individuals' privacy concerns, whereas perceived vulnerability increased privacy concerns (Dinev & Hart, 2004). The privacy calculus used by Dinev and Hart (2004) essentially emphasized how individuals' perceptions were formed when contrary but salient factors were present.

Following the study by Dinev & Hart (2004), an extended privacy calculus model was developed and tested in the context of online transactions (Dinev & Hart, 2006). The extended privacy calculus posited that when individuals undergo situations whereby they are required to disclose their personal information, a calculus of risk beliefs, as well as confidence and enticement beliefs existed (Dinev & Hart, 2006). Among the risk beliefs were privacy risk and privacy concerns, which, were both found to negatively influence individuals' personal information disclosure. Likewise, Dinev and Hart (2006) included trust and personal internet interest as the confidence and enticement beliefs, and found that they both positively influenced individuals' disclosure of personal information. The findings of Dinev and Hart (2006) were consistent with that of studies whereby trust influenced personal information disclosure (Bansal et al., 2010; Malhotra et al., 2004). Similarly, Dinev and Hart's (2006) findings of privacy risk's negative impact on an individual's personal information disclosure corroborated with the findings of prior research, such as that of Malhotra et al. (2004).

The privacy calculus is adaptable to multiple definitions of privacy. For instance, while the most apparent definition (based on the extended model) is that of a commodity-based definition (Dinev & Hart, 2006; Smith et al., 2011), it has been adopted by a number of researchers, and in some instances has been aligned with a control-based definition (Dinev & Hart, 2004; Xu, Dinev, Smith, & Hart, 2008; Xu et al., 2010; 2012). However, the privacy calculus assumed that individuals were rational in their decision-making (Dinev & Hart, 2006). This assumption was consistent with a number of other studies which assumed that there existed some rational process behind individuals' personal information disclosure (Acquisti & Varian, 2005; Awad &Krishnan, 2006; Culnan & Armstrong, 1999; Pavlou et al., 2007; Van Slyke et al., 2006), thereby neglecting the emotional and situational aspects of individuals' decision-making (Li et al., 2011).

2.4.2. Debates that Privacy-Related Decisions Are Not Purely Rational

According to Acquisti (2004), individuals are unable to make purely rational decisions with regards to privacy concerns due to 'bounded rationality'. Specifically, individuals do not possess all the information of the parameters governing a given situation (Acquisti & Grossklags, 2005). Moreover, even if the individual had all the information required for a rational decision, his/her cognitive ability would be limited in the processing of all this information (Acquisti, 2004). Therefore, studies have examined other arguments to better explain individuals' privacy decisions (Acquisti, 2004; Angst & Agarwal, 2009; Li et al., 2011). Acquisti (2004) proved that a number of psychological distortions may be enacted when individuals make decisions concerning their information privacy, such as hyperbolic discounting of future costs and benefits. As such, individuals' decisions of privacy may be affected by their estimations which differ at different points of time, which may lead to individuals having faulty assessments and undermining their risks (Acquisti, 2004).

Studies also found psychological features contributed to individuals' perceptions of privacy and decisions to provide or withhold personal information (Acquisti & Grossklags, 2005; Bansal et al., 2010). In their study, Bansal et al. (2010) found personality differences affected individuals' privacy-related decisions, along with positive factors (such as trust and prior positive experiences), and negative factors of risk beliefs, prior online invasions and privacy concerns. Acquisti and Grossklags (2005) found that incomplete information, bounded rationality and systemic psychological deviations (such as overconfidence in risk assessments), affected individuals' privacy-related decision making.

Consistent with explaining the privacy-paradox based on psychological arguments that discounted a purely rational perspective, Li et al. (2011) argued that various situational factors affected individuals when they interact with a website. Due to the situational factors, privacy-related decision-making is dynamic (Li et al., 2011). Essentially, despite any preconceptions an individual may have with regards to disclosing their personal information, situational factors would influence their behavior. As such, Li et al. (2011) adopted the stimulus-organism-response (S-O-R) model, whereby the affective and cognitive states of an individual is based on the environment. Emotions, such as joy or fear incorporated the affect-based state, whereas the cognition-based state comprised of perceived relevance of information and awareness of privacy statements. Li et al. (2011) posited that the affective and cognate states had an impact on the privacy calculus which individuals undergo. While Li et al. (2011) found that individuals' privacy concerns shaped their privacy beliefs; initial emotions (affect-based state) and fairness levers (cognate-based state) were also influential to privacy beliefs and subsequently, individuals' decisions to disclose personal information. In essence, the study by Li et al. (2011) corroborated the arguments that individuals' privacy behavior was not purely rational.

Anderson and Agarwal (2011) further improved the explanatory power of the privacy calculus with regards to the privacy paradox by including emotions as a necessary factor for consideration. Anderson and Agarwal (2011) argued that the examination of privacy concerns within the healthcare context need to differ from previous privacy studies since there exists a “consideration of risk that is substantially more granular than has been explored in past privacy studies” (p. 471). As such, emotions played a significant role in influencing individuals’ decisions to disclose their personal information (Anderson & Agarwal, 2011). Their findings suggested that the emotions individuals perceive over their health status influenced them to disclose or withhold their personal information, however, so did the privacy calculus, which consisted of trust and privacy concerns (Anderson & Agarwal, 2011). While the findings of Anderson and Agarwal (2011) differed from Li et al. (2011) in that emotion influenced individuals to disclose their personal information directly, and not the privacy calculus; essentially, a major contribution from their study was that individuals’ decision making could be dominated by emotional states as opposed to being purely rational. Despite the argument of Anderson and Agarwal (2009) that privacy within the healthcare context needed to be studied differently, their findings lent support to the debates that emotions need to be considered along with rationality when examining individuals’ privacy behaviors, despite the context.

2.5. Summary

Information privacy is a subset of the general field of privacy, which has been defined by researchers as either a value or cognate-based (Smith et al., 2011). Specifically, privacy is defined as a value as a human right or a commodity that could be traded for something in return. Privacy as a cognate-based definition, however, refers to the subjective value an individual place over the privacy of their personal information, and may be regarded as either a cognitive state or control (Smith et al., 2011). The definitions of information privacy have allowed researchers to develop theoretical research models for empirically examining the privacy paradox, which is the contradictory actions of individuals who claim concerns for information privacy, but continue to disclose their personal information (Dinev & Hart, 2004; 2006; Norberg et al., 2007; Van Slyke et al., 2006). The privacy calculus has often been used to explain the privacy paradox (Laufer & Wolfe, 1977; Dinev & Hart, 2006), which assumes that individuals make decisions rationally. Yet, individuals are not purely rational decision-makers (Acquisti & Grossklags, 2005). Studies have therefore integrated emotions as key factors in individuals' privacy-related decision-making (Anderson & Agarwal, 2011; Li et al., 2011). Essentially, a better understanding of the privacy paradox could be achieved by considering both the rationality and emotional thought processes behind individuals' privacy-related decisions.

Chapter 3

Theory

3.1. Introduction

This chapter consists of the theory used for the development of the research model and hypotheses for this study. Section 3.2 presents the theory used for this study, how it was expanded upon using cognitive neuroscience, as well as relevant information of the neuroanatomy of the human brain to better understand how cognitive neuroscience is used to better explain the privacy paradox. Section 3.3 presents an overarching research model for the study, along with the hypotheses, and their separate models. Section 3.4 then summarizes and ends the chapter.

3.2. Theoretical Basis

The privacy calculus has often been used to explain individuals' privacy-related decisions, particularly in understanding the privacy paradox, positing that individuals' would trade their personal information based on a cost-benefit analysis (Culnan & Bies, 2003; Dinev & Hart, 2004; Laufer & Wolfe, 1977, Smith et al., 2011). The principles of the privacy calculus have often been adopted by researchers greatly in extant literature in the information privacy field (Bansal et al., 2010; Dinev & Hart, 2004; 2006; Dinev et al., 2006; Li et al., 2011; Malhotra et al., 2004; Xu et al., 2010). Essentially, researchers have often explained the privacy paradox using the privacy calculus, highlighting the numerous cost-related and benefit-related factors that influence privacy-related decisions. For instance, in their study, Dinev and Hart (2006) found factors of trust and personal interest (benefits) acted against factors of privacy concerns and privacy risk (costs) in individuals’ decisions to disclose personal information.

The privacy calculus is limited in assuming individuals are purely rational decision makers, yet, researchers have recognized the need to include emotions in investigating individuals' privacy-related decisions (Anderson & Agarwal, 2011; Li et al., 2011). Following the studies that sought to gain a better understanding of the privacy paradox, this study adopted the extended privacy calculus model developed by Dinev and Hart (2004) as the theoretical basis. However, the extended privacy calculus model is limited in the assumption that individuals are purely rational decision-makers. To address this limitation, the findings from cognitive neuroscience were applied to the extended privacy calculus model. The introduction of cognitive neuroscience thus enhanced the explanation provided by the extended privacy calculus model in interpreting the privacy paradox.

3.2.1. Extended Privacy Calculus Model

This study used the extended privacy calculus model developed by Dinev and Hart (2006), as the basis for the research model. Despite the limitations of the privacy calculus in assuming individuals’ decisions are purely rational, it greatly contributes to explaining the privacy paradox. The cost-benefit tradeoff has been adopted by many researchers with regards to personal information disclosure, most often including privacy risk beliefs, trusting beliefs and other contrary but influential factors (Bansal et al., 2010; Dinev & Hart, 2004; 2006; Li et al., 2011; Malhotra et al., 2004; Norberg et al., 2007; Xu et al., 2010).

Depicted in Figure 1, the extended privacy calculus model posited that individuals' intentions to disclose personal information were inhibited by privacy risk and privacy concerns, but influenced by trust and personal interest (Dinev & Hart, 2006). Privacy risk was defined as the risk of opportunistic behavior towards the personal information an individual disclosed, which was associated with the possibility of loss and uncertainty (Dinev & Hart, 2006). Privacy risk correlated positively with privacy concern, but negatively with trust (Dinev & Hart, 2006). Essentially, if an individual perceived more trust in disclosing his/her personal information, his/her perception of privacy risk would be lower. Trust was one of the confidence and enticement beliefs, which positively influenced individuals' intentions to disclose personal information. Personal interest is the other confidence and enticement belief factor that was defined as the intrinsic motivation toward performing an action, and the satisfaction derived from doing so (Dinev & Hart, 2006).

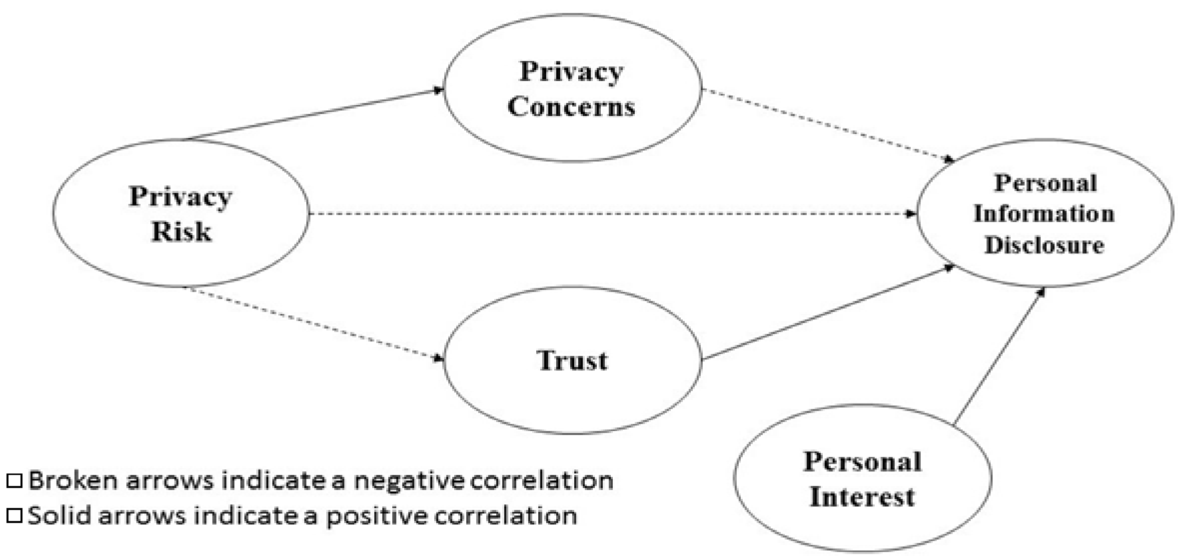


Figure 1. Extended Privacy Calculus Model developed by Dinev & Hart (2006)

3.2.2. Using Insights from Cognitive Neuroscience to Enhance the Extended Privacy Calculus

Acquitsi and Grossklags (2005) explained that privacy-related decisions may be limited by bounded rationality, and cognitive biases. Specifically, Acquisti (2004) explained the cognitive bias of hyperbolic discounting as a cause for individuals' decisions to disclose personal information despite claiming concerns for their information privacy. Essentially, individuals would prefer short-term benefits rather than the better choice of long-term benefits (Acquisti, 2004). However, explaining the privacy paradox by arguing for the saliency of cognitive biases, such as hyperbolic discounting, ignores the rational aspects involved in privacy-related decisions. While individuals' disclosure of personal information may not be purely rational, findings from cognitive neuroscience have explained that decisions are complex enough to involve multiple mental processes (Dimoka et al., 2007).

Findings of cognitive neuroscience indicated that there are correlations between mental processes and specific brain areas. Rational cognitive processes are often correlated with brain activity in the prefrontal cortex, while emotions are often correlated with the limbic system (Dimoka et al. 2007). Furthermore, these systems of rationality (prefrontal cortex) and emotional processing (limbic system) interact with one another (Phelps, 2006). Essentially, no decision is purely rational, nor is any decision purely emotional. Furthermore, Dimoka (2012) explained that individuals' brain activity does not necessarily mean that only one mental process is occurring. There exists a many-to-many relationship between brain activity and mental processes (Dimoka, 2012). For instance, when an individual perceives some activity will yield specific rewards, several key brain areas are activated, such as the orbitofrontal prefrontal cortex, medial prefrontal cortex, amygdala, nucleus accumbens, and caudate nucleus (Dimoka et al., 2007). The brain areas activated in assessing rewards include areas present in both the prefrontal cortex and the limbic system (Dimoka et al., 2007). Therefore, to elicit a better understanding of the privacy paradox, it would be essential to observe how individuals decide to withhold or disclose their personal information.

Cognitive neuroscience provides a number of tools and techniques to measure individuals' brain activity, and associate brain functions with mental processes. Popular within brain mapping literature, is the use of the functional magnetic resonance imaging (fMRI) scanner to track the flow of oxygenated and deoxygenated blood to specific brain areas (Dimoka, 2012; Riedl et al., 2009). Yet, many studies in cognitive neuroscience have used the electroencephalogram (EEG) to track individuals' electrophysiological responses. These electrophysiological responses are electric potentials produced from neurons within the brain, and is categorized by different frequency bands (Guyton & Hall, 2001). These frequencies, measured in Hertz (Hz), correspond to a variety of functions (Demos, 2005). The frequency bands and their associated functions are summarized from Demos (2005) in Table 1.

Table 1. Frequency bands of electric potentials

Waves	Frequency	Function
Delta waves	1-4	Produced more in infants and children than adults, and pertains to the functioning of the immune system, natural healing, and deep sleep.
Theta waves	4-8	Connected to feelings of deep and raw emotions. High frequencies of theta waves are associated with depression,

		impulsivity, hyperactivity, and inattentiveness. Low frequencies of theta waves are associated with anxiety, poor emotional awareness, and stress. Optimal frequencies of theta waves are associated with intuition, relaxation, creativity and emotional connection.
Alpha waves	8-12	The state between the conscious and subconscious mind, often produced in resting state, with eyes closed. High frequencies of alpha waves relate to daydreaming, excessive relaxation, and the inability to focus. Low frequencies of alpha waves relate to anxiety, high stress, insomnia, and obsessive-compulsive behavior. Optimal levels of alpha waves pertain to relaxation.
Beta waves	13-21	Relates to conscious thought, logical thinking, focus and problem solving.
High Beta waves	20-32	Pertains to intensity, anxiety and hyper alertness.
Gamma waves	38-42	Involved in higher processing tasks and cognitive functioning.

While the extended privacy calculus model (Dinev & Hart, 2006) consisted of privacy risk, privacy concern, trust and personal interest, cognitive neuroscience has found these factors correlated with neural activity in specific areas of the brain. Different brain areas are responsible for different functions, such as motor control, executive functions, and emotional processing. Thus, these brain areas associated with the mental processes or factors involved in the extended privacy calculus enhances the investigation of individuals’ privacy-related decisions. Furthermore, other factors such as uncertainty and distrust are important in considering since uncertainty was found to be an antecedent of personal information disclosure (Pavlou et al., 2007), and distrust as a distinct factor from trust (Dimoka, 2010). Thus, the findings of cognitive neuroscience were applied to the extended privacy calculus model, to elicit a better explanation of the privacy paradox, identifying both the involvement of emotions and rationality in individuals' privacy-related decisions.

3.2.3. Neuroanatomy – Structure and Function of Key Brain Areas

Adequately applying the findings of neuroscience to the field of Information Systems to better understand IS problems, require a basic understanding of the structure of the human brain (i.e. its anatomy), as well as some key functions of these brain areas. The human brain is part of the central nervous system, which consists of gray and white matter, and are divided into three principle areas, the forebrain, midbrain and hindbrain. The gray matter are nerve cells, called neurons, while the white matter are axons, which are linked to the neurons for neuronal communication (Demos, 2005; Hanaway, Woosley, Gado, & Mellville, 1998; Snell, 2010). Connected to the spinal column is the hindbrain, which contains the medulla oblongata, pons, and cerebellum, with the midbrain connecting the hindbrain to the forebrain (Snell, 2010). The forebrain consists of the telencephalon and diencephalon. The telencephalon is composed of the cerebrum, separated into a right and left hemisphere, composed of an outer layer, known as the cerebral cortex, and subcortical structures such as the basal ganglia (Cannon, 2012; Demos, 2005). The diencephalon is the inner part of the forebrain consisting of the thalamus and hypothalamus. The diencephalon is comprised mainly of gray matter, and is situated at the head of the brain stem, thus linking lower brain stem structures to the cerebral cortex (Cannon 2012). The cerebral hemisphere is partitioned into four lobes: the frontal lobe, temporal lobe, parietal lobe, and occipital lobe. Each hemisphere consists of a number of bulges, known as gyri (pl. gyrus), and small and large grooves known as sulci (pl. sulcus) and fissures, respectively (Goldberg, 2010). As depicted in Figure 2, the frontal lobe is the anterior part of the brain, the temporal lobe is located to the side, and the parietal lobe is behind the frontal lobe, but above the occipital lobe. The occipital lobe, which is located at the base of the brain, is primarily associated with vision (Demos, 2005).

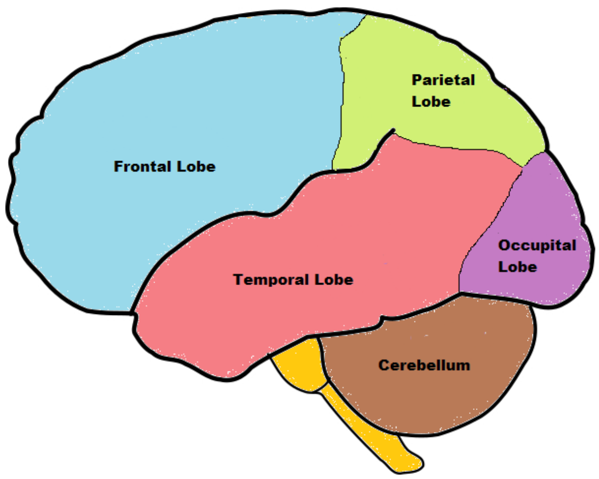


Figure 2. Lobes of the Cerebral Cortex

Further division of the cerebral cortex into specific areas was developed by Korbinian Brodmann in 1908 into a cytoarchitectural map consisting of Brodmann Areas (BA) labeled 1 to 52 (Cannon, 2012). The BA's were developed based on the organization of neurons, and have since been the most widely accepted cytoarchitectural map of the cerebral cortex, which, over the years, have undergone re-evaluations and further divisions (Cannon, 2012). BA's are responsible for many different functions ranging from somatosensory perceptions, such as temperature and pain, located in BA's

1, 2, and 3 (also known as the Somatosensory Cortex), to decision-making, which is located in BA 8. Brodmann areas exist in both hemispheres. For instance, there are right and left BA 5's. Figure 3a and 3b depicts the Brodmann Areas within the brain, while table 2 illustrates some of the functions found to be associated with these Brodmann Areas.

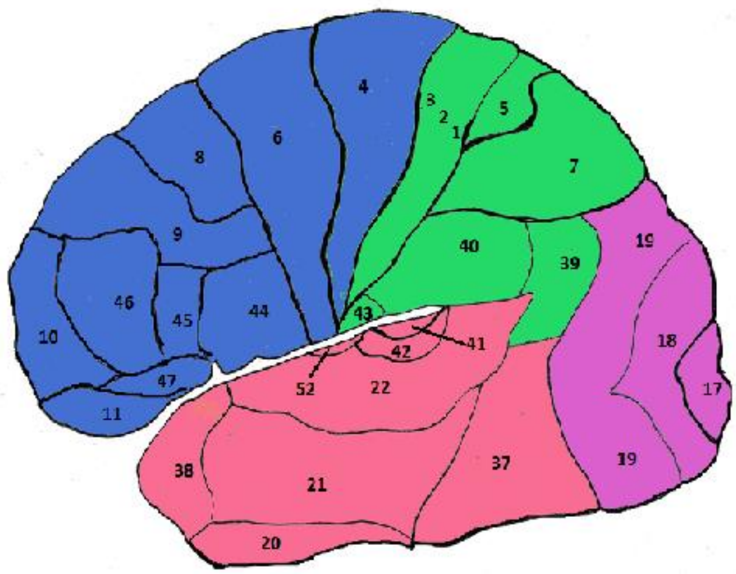


Figure 3a. Brodmann Areas of the Cerebral Cortex (outer view)

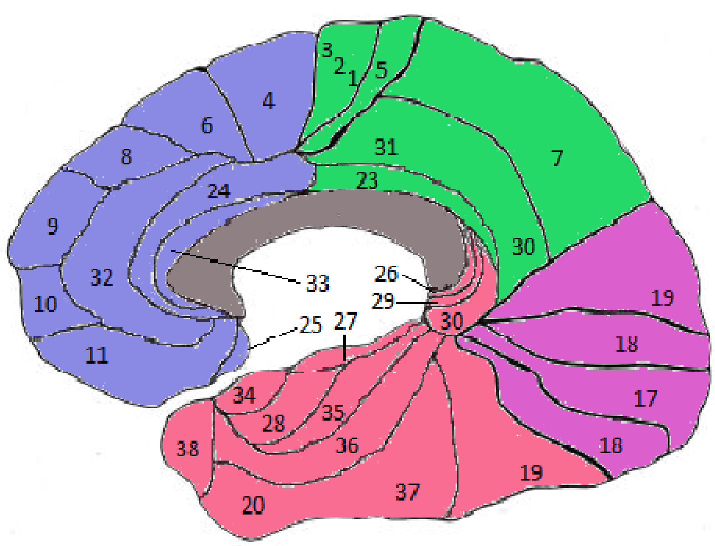


Figure 3b. Sagittal View of Brodmann Areas in the Brain

Table 2. Brief overview of Brodmann Areas and some of their Associated Functions

Brodmann Areas	**Name of Areas**	**Functions**	**References**
1, 2, 3	Postcentral Gyrus	Temperature, pain, proprioception and nociception processes	Kirimoto, Ogata, Onishi, Oyama, Goto, & Tobimatsu (2010); McCaslin, Chen, Radosevich, Cauli, & Hillman (2010); Straube & Miltner (2011); Zhang, Jiao, & Sun (2011)
4 & 6	Premotor Cortex	Motor functions	Luria (1966)
5 & 7	Superior Parietal Lobule	Motor execution, spatial imagery in deductive reasoning	Knauff, Mulack, Kassubek, Salih, & Greenlee (2002); Stephan, Fink, Passingham, Silbersweig, Ceballos-Bauman, Frith, & Frackowiak (1995)
8, 9, 10	Prefrontal Cortex	Decision-making, uncertainty, executive attention, self-regulation, emotion, arithmetic processes	Cannon, Congedo, Lubar, & Hutchens (2009); Cannon, Sokhadze, Lubar, & Baldwin (2008); Jahanashi, Dirnberger, Fuller, & Frith (2000); Volz, Schubotz, & von Cramon (2005)
11, 12, 25	Orbitofrontal Cortex	Emotional regulation, self-regulation, encoding and retrieval, decision-making involving rewards	Cannon (2012); Ernst et al. (2004)
13, 14, 15, 16	Insular Cortex	Fear, risk-taking	Phelps, O'Connor, Gatenby, Gore, Grillon, & Davis (2001); Paulus & Frank (2003)
17, 18, 19	Primary & Secondary visual cortices	Associated with vision	Cannon (2012)
20, 21, 22	Inferior Temporal, Fusiform & Parahippocampal Gyri	Attribution of attention to others	Brunet, Sarfati, Hardy-Bayle, & Decety (2000)

23, 26, 29, 30, 31	Posterior Cingulate Gyrus	Emotions and episodic memory processes	Cannon (2012)
24, 25, 32, 33	Anterior Cingulate Gyrus	Consciousness, learning, reward, and decision-making	Devinsky, Morrell, & Vogt (1995)
27, 28, 34, 35, 36, 48	Hippocampal Areas	Emotional memories, fear	Reinders, Gascher, de Jong, Willemsen, den Boer, & Buchel (2006); Richardson, Strange, & Dolan (2004).
37	Fusiform Gyrus	Visual recognition	Tanaka (1997)
38	Temporal Pole	Social and emotional processes, decision-making	Dupont (2002)
39	Angular Gyrus	Integration of visual and tactile stimuli in addition to speech	Cannon (2012)
40	Supramarginal Gyrus	Writing of single letters	Rektor, Rektorova, Mikl, Brazdil, & Krupa (2006)
41 & 42	Primary Auditory Cortex	Basic auditory processing	Stefanatos, Joe, Aguirre, Detre, & Wetmore (2008)
43	Subcentral Area	Sign and spoken language	Soderfeldt, Ingvar, Ronnberg, Eriksson, Serrander, & Stone-Elander (1997)
44 & 45	Broca’s Area	Involved in the production of language	Cannon (2009)
46	Anterior Middle Frontal Gyrus	Processing emotions and self-reflections in decision-making (left)	Deppe, Schwindt, Kugel, Plassman, & Kenning (2005)
47	Inferior Frontal Gyrus	Decision making involving conflict and rewards (right)	Rogers, Own, Middleton, Williams, Pickard, Sahakian, & Robbins (1999)

3.3. Research Model

The research model is based on the application of the findings of cognitive neuroscience to the extended privacy calculus model developed by Dinev and Hart (2006). The privacy calculus has often been used by researchers to study the beliefs individuals have concerning the disclosure of their personal information in various contexts, such as ecommerce, ehealth, social media, and profiling (Awad & Krishnan, 2006; Bansal et al., 2010; Dinev & Hart, 2006), due to the influence certain factors, such as trust and risk. However, a distinction should be made between the oft-measured beliefs, when researchers use the privacy calculus, and the perceptions or mental processes identified in this study.

Factors such as risk beliefs and trust beliefs, often used in the literature (Dinev & Hart, 2006; Li et al., 2011), pertains to an individuals' enduring perceptions or beliefs of a given situation. However, individuals' attitudes (i.e. their perceptions or mental processes) may be different due to situational factors and cognitive limitations (Acquisti & Grossklags, 2005; Belanger & Crossler, 2011; Sim et al., 2012), often triggered by some stimuli. Specifically, the extended privacy calculus model developed by Dinev and Hart (2006) identified a number of salient factors (such as trust and risk) present in privacy-related decisions. While these factors were measured as beliefs, research in cognitive neuroscience has identified these factors as mental processes, which may be derived from a both internally held beliefs and external stimuli (Angst & Agarwal, 2009; Dimoka, 2010; 2012; Dimoka et al., 2007; Li et al., 2011). Additionally, factors of uncertainty and distrust were added to the privacy calculus based on the findings of cognitive neuroscience that these factors were distinct from factors such as risk or trust

(Dimoka, 2010; Dimoka et al., 2007; 2011). Specifically, Dimoka (2010) found distrust was associated with brain areas different from the brain areas associated with trust. Figure 4 presents the overarching research model for this study developed from the extended privacy calculus and pertaining to the mental processes predicting privacy concerns and personal information disclosure. This model is further broken in the next two subsections, displaying the inclusion and relationships between these mental processes and brain areas in predicting privacy concerns and personal information disclosure.

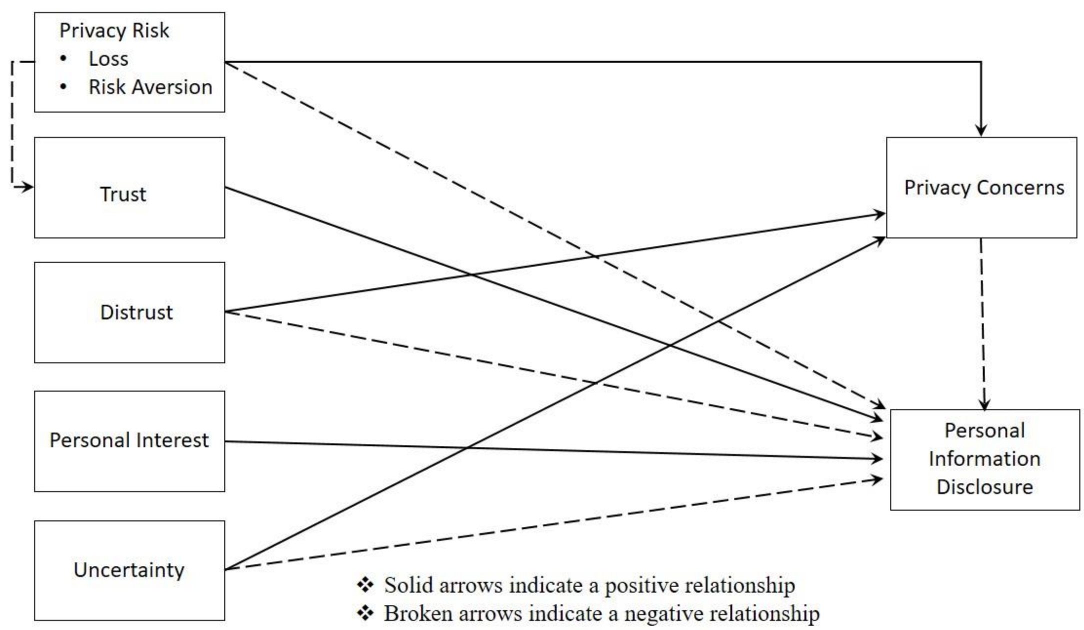


Figure 4. Overarching research model

3.3.1. Hypotheses Development – Neural Correlates

The following hypotheses were developed mainly from research using positron emission tomography (PET) scans and fMRI techniques for source localization.

Localization of brain activity may not be the same across neuroimaging technologies; however, past research can provide an idea as to where neural activity may take place in specific situations. Thus, these hypotheses are developed more as a guideline to where brain activity might occur. Specifically, exploring neural activity for specific mental processes might produce varied results from past literature based on a number of factors such as the design of experiments and neuroimaging tools selected. As explained by Cannon (2012), the brain is a complex system of systems, whereby findings in current neuroscience literature can be challenged as new findings can refute previous understanding of the brain. Figure 5 depicts the hypotheses of brain areas correlated with the mental perceptions of the extended privacy calculus model.

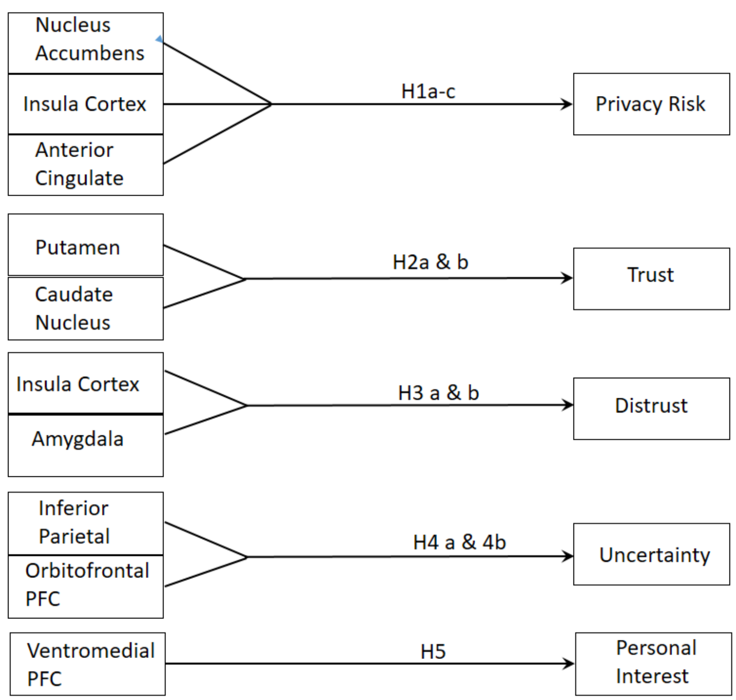


Figure 5. Neural Correlates of Mental Processes

Researchers in the field of information privacy have often treated privacy risk as a one-dimensional construct (Dinev & Hart, 2006; Malhotra et al., 2004; Norberg et al., 2007; Smith et al., 2011). However, privacy risk may actually be a multidimensional construct whereby an individual's perception of risk may assess the likelihood and severity of consequences in engaging or avoiding a risky action (Peter & Tarpey, 1975; Smith et al., 2011). Privacy risk is essentially an individual's perception of risk but in the context of information privacy. According to Dinev and Hart (2006), privacy risk wis defined as the possibility of loss, which is related to the uncertainty caused by the possibility of harm to the individual if he/she were to disclose his/her personal information. 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, Fong, Adams, Varner, & Hommer, 2001), is activated when individuals sought to avoid risky behavior (Matthews, Simmons, Lane, & Paulus, 2004). However, brain activity in the insular cortex correlated with risky games when individuals perceived high loss predictions (Paulus & Frank, 2003). Additionally, Brown and Braver (2007) indicated that the anterior cingulate cortex might be involved in avoiding risks. Similarly, Massar, Rossi, Schutter, and Kenemans (2012) found that individuals with high behavioral inhibition system (BIS) scores (i.e. an assessment of punishment severity) had a high theta/beta ratio correlated with low feedback related negativity (a component of an event-related potential), whereby the baseline theta activity was generated in the anterior cingulate cortex.

H1a: *Privacy Risk is associated with brain activity in the nucleus accumbens.*

H1b: *Privacy Risk is associated with brain activity in the insula cortex.*

H1c: *Privacy Risk is associated with brain activity in the anterior cingulate cortex.*

The extended privacy calculus model found trust to be a salient factor that positively influenced individuals to disclose their personal information (Dinev & Hart, 2006). Trust is defined as the confidence of an individual that organizations would act benevolently in protecting them from harm caused by the personal information they collect (Dinev & Hart, 2006). The extended privacy calculus model neglected the impact of distrust because researchers have often assumed that trust and distrust lay at opposite ends of a single continuum (Dimoka, 2010). However, Dimoka (2010) found that trust correlated with brain activity in the caudate nucleus and putamen, whereas distrust correlated with the amygdala and insular cortex (Dimoka, 2010). These findings indicated that trust and distrust are distinct from each other. Moreover, the effect of distrust was more influential than trust when subjects made decisions about price premiums (Dimoka, 2010).

H2a: *Trust is associated with brain activity in the caudate nucleus.*

H2b: *Trust is associated with brain activity in the putamen.*

H3a: *Distrust is associated with brain activity in the amygdala.*

H3b: *Distrust is associated with brain activity in the insula cortex.*

Studies in neuroscience found uncertainty correlates with the orbitofrontal cortex and inferior parietal cortices (Krain, Wilson, Arbuckle, Castellanos, & Milham, 2006), which are different from the neural correlates in risky situations. Pfeffer and Salancik (1978) explained uncertainty as the inability to accurately anticipate the future state of a situation because of a lack of enough information. Specifically, when using ICTs, such as ecommerce, uncertainty may exist when an individual is unsure of the outcome if he/she were to disclose his/her personal information. This is often due to a lack of information regarding the parameters of such a situation, such as the case with buyers and sellers in ecommerce transactions (Acquisti, 2004; Pavlou et al., 2007). Yet, uncertainty is different from ambiguity and risk. An individual may be privy to a great deal of information when deciding to disclose his/her personal information, and may assess the situation as risky. Alternatively, ambiguity is not necessarily considered as negative, as opposed to risky or uncertain situations (Krain et al., 2007).

H4a: *Uncertainty is associated with brain activity in the orbitofrontal prefrontal cortex.*

H4b: *Uncertainty is associated with brain activity in the inferior parietal cortex.*

In the extended privacy calculus model, personal interest is defined as an enticement that would influence individuals to disclose personal information (Dinev & Hart 2006). This may be based on an individual's intrinsic motivation to use a system despite the requirement to disclose his/her personal information and the risk associated with doing so. This decision may not be altogether rational, but rather impulsive as suggested in the findings of Belanger et al. (2002), where individuals preferred the pleasure of online shopping to security and privacy. In a similar manner to the impulsivity of consumer behavior, personal interest was assumed to be associated with the similar cognitive processes of high activations in the ventromedial prefrontal cortex and inferior parietal lobule (right BA 40), but low activations in the dorsolateral prefrontal cortex (Deppe et al., 2005).

H5a: *Personal Interest is associated with high brain activity in the ventromedial prefrontal cortex, but low activity in the dorsolateral prefrontal cortex.*

H5b: *Personal Interest is associated with brain activity in the inferior parietal lobule.*

3.3.2. Hypotheses Development – Relationship with Privacy Concerns and Personal Information Disclosure

Dimoka (2010) found that the neural activity of brain areas correlated with perceptions of trust and distrust provided a better explanation to decisions of price premiums than psychometric data. Similarly, the neural activity of brain areas correlated with the perceptions of privacy risk, trust, distrust, uncertainty and personal interest should be better predictors than self-reported data. Thus, the following hypotheses were formed on the basis that neural correlates of the predictors of the extended privacy calculus would influence individual's perceptions of privacy concerns, as well as their decisions to withhold or disclose their personal information.

In the extended privacy calculus model, privacy risk influenced privacy concerns, while inhibiting personal information disclosure (Dinev & Hart, 2006). Privacy risk has been seen in a number of studies as an inhibitor to personal information disclosure (Malhotra et al., 2004; Norberg et al., 2007; Van Slyke et al., 2006). However, privacy risk may be more complicated than past studies have suggested, as it may entail both the perceptions of loss, as well as the anticipation of outcomes if a risky action were averted. Furthermore, findings in neuroscience suggest that risky situations involve brain areas that are involved in strong negative emotions (such as the insula cortex) as well as reward centers (Knuston et al., 2001; Paulus & Frank, 2003). While the full extent of the role privacy risk may be unknown in relation to privacy-related situations, the following hypothesis was developed based on findings from prior literature.

H6a: *The neural correlates for privacy risk are positively related to privacy concerns.*

H6b: *The neural correlates for privacy risk are negatively related to personal information disclosure.*

The extended privacy calculus model found that high levels of risk were negatively related to high levels of trust (Dinev & Hart, 2006). Similarly, the neural correlates of risk and trust may have a negative relationship. Trust was found to positively influence personal information disclosure (Dinev & Hart, 2006; Pavlou et al., 2007; Van Slyke et al., 2006). However, as trust and distrust were found to be distinct from each other with regards to their neural correlates, it is expected that both the neural correlates of distrust and trust would have some influence on personal information disclosure. Additionally, in the same manner that privacy risk, which has been considered as a negative construct in previous studies (Dinev & Hart, 2006; Malhotra et al., 2004; Van Slyke et al., 2007), has a relationship with privacy concerns, it is also expected that the neural correlates of distrust may enforce individuals' privacy concerns.

H7a: *The neural correlates of privacy risk are negatively related to the neural correlates of trust.*

H7b: *The neural correlates of trust are positively related to personal information disclosure.*

H8a: *The neural correlates of distrust are positively related to privacy concerns.*

H8b: *The neural correlates of distrust are negatively related to personal information disclosure.*

The extended privacy calculus model by Dinev and Hart (2006) found personal interest directly influenced individuals to disclose their personal information. Similarly, the neural correlates associated with personal interest should be related to individuals' decisions to disclose their personal information. Similarly, perceptions of uncertainty, and the associated neural correlates would increase privacy concerns, while inhibiting personal information disclosure. Specifically, in the context of information privacy, uncertainty is often considered negative, which may be related to privacy concerns (Pavlou et al., 2007). 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 also influence individuals to withhold their personal information.

H9: *The neural correlates of personal interest are positively related to personal information disclosure.*

H10a: *The neural correlates of uncertainty are positively related to privacy concerns.*

H10b: *The neural correlates of uncertainty are negatively related to personal information disclosure.*

Privacy concerns are often used in information privacy field as an appropriate measure of information privacy (Smith et al., 2011). Dinev & Hart (2006) defined privacy concerns as the concerns an individual has over the opportunistic behavior of another entity to which an individual would disclose his/her personal information. Dinev and Hart (2006) distinguished privacy risk from privacy concerns by explaining that privacy risk was a perception based on the individual's overall perception of disclosing his/her personal information, while privacy concerns was an internalization of what happens to the personal information the individual has disclosed. Studies have often categorized privacy concerns as a multi-dimensional construct reflecting dimensions of concerns for the collection, unauthorized secondary use, improper access and errors of personal information (Smith et al., 1996; Stewart & Segars, 2002). The IUIPC asserted that the dimensions of privacy concerns in the era of the internet were based on the concerns for the collection and control of personal information, as well as the individual's awareness of how the personal information he/she has disclosed to an entity is handled. It is assumed that the greater an individual's degree of privacy concerns, the more likely he/she would withhold his/her personal information. Figure 6 depicts the research model that was tested in the study (except for hypothesis 12).

H11: *Privacy Concerns are negatively related to personal information disclosure*

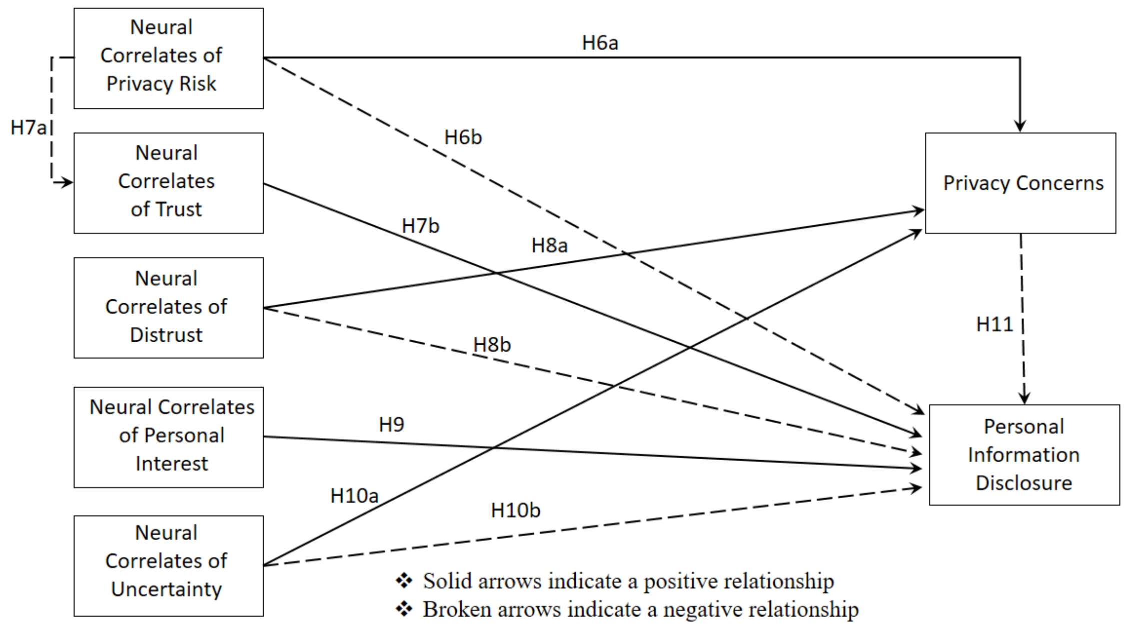


Figure 6. Research Model Depicting Hypothesized Relationships

Based on the findings of cognitive neuroscience, the constructs or mental processes that are involved in individuals' privacy concerns, as well as their decision to disclose their personal information are distinct (Dimoka et al., 2007). As found by Dimoka (2010), a high level of trust does not dictate that a low level of distrust would be perceived by an individual. In the same manner that both distrust and trust can be perceived at the same time and at varying degrees (Dimoka, 2010), individuals may perceive other mental processes such as risk and personal interest at the same time and at varying degrees. However, the effect of an independent variable on the dependent variable can be changed due to the presence of other independent variables. These effects are referred to as interaction effects. It should be noted that the following hypotheses on interaction effects are not represented in the research model, since interaction effects should not alter the direction of the relationships between the independent variables and the dependent variables. For instance, the interaction effects would not alter hypotheses such as 6b, which posits that risk would negatively influence personal information disclosure, but would determine the amount of change in the dependent variable based on the interactions between independent variables.

H12a: *An interaction effect would exist between the independent variables (privacy risk, trust, distrust, personal interest, uncertainty) and privacy concerns.*

H12b: *An interaction effect would exist between the independent variables (privacy risk, distrust, personal interest, uncertainty, privacy concerns) and personal information disclosure.*

3.4. Summary

The extended privacy calculus model developed by Dinev and Hart (2006) was used as the theoretical basis for this study. However, the extended privacy calculus model is limited in assuming individuals are purely rational decision-makers. To address this limitation, the findings of cognitive neuroscience were added to the extended privacy calculus. The findings of cognitive neuroscience aid in identifying the neural correlates of mental processes, which predict individuals' privacy-related decisions. Identifying these neural correlates allow for examining the nature of these mental processes (such as rational and/or emotional) as well as observes the relationships between these mental processes in privacy-related decisions.

Chapter 4

Research Design

4.1. Introduction

This chapter consists of the research design used for testing the research model and hypotheses for this study. Section 4.2 presents the research method used, while section 4.3 explains how the data was collected. Section 4.4 details the design of the research method to adequately capture data for analysis and achieving the objectives of this study. Section 4.5 explains the data analysis, including the preprocessing of data before analysis. Section 4.6 concludes the chapter with a summary.

4.2. Research Method

Three within-subject experiments were conducted using an EEG device to measure subjects' brain activity. All subjects participated in the three experiments as if it were one experiment, while the conditions associated with each experiment were later separated and analyzed accordingly. Experiments were chosen as the selected research method, as it allows researchers to control the environment through manipulations (i.e. treatments or conditions) to observe specific behavior, and retain strong internal validity (Sekaran & Bougie, 2013). However, experiments are often used for examining causal relationships (Sekaran & Bougie, 2013), yet, inferring a causal relationship between mental processes and research constructs can lead to erroneous assumptions, referred to as "reverse inference" (Poldrack, 2006). This is because there exists a many-to-many relationship between mental processes and brain activity, whereby a research construct, such as trust, may generate brain activity in multiple regions of the brain, while another construct may generate activity in similar brain regions (Dimoka, 2012). However, experiments using an EEG expose subjects to treatments, where data is recorded and analyzed, and a conclusion can be drawn over the neural correlates associated with specific mental processes and certain decisions. It should be noted, however, that as the brain is considered extremely complex with multiple sub-systems, whatever results are discovered in current studies can easily be challenged with newer neuroimaging tools and techniques, resulting in vastly different results that are more accurate (Cannon, 2009).

EEG captures brain activity through electrodes which detect the voltage fluctuations on the scalp which "results from the changes in membrane conductivity elicited by synaptic activity and intrinsic membrane processes" (Riedl et al., 2009, p. 246). While EEG provides lower spatial resolution in comparison to neuroimaging technology such as fMRI and PET, it provides a high temporal resolution, where brain activity is captured in milliseconds (Riedl et al., 2009), and epochs are extracted from continuous records for thorough analysis of event-related potentials. This lack of spatial resolution leads to the "inverse problem", whereby the location of origination of neural activity is often too ambiguous to identify (Grech et al., 2008). However, this inverse problem can be addressed using a number of mathematical formulations such as the low-resolution electrical tomography (LORETA) and the standardized LORETA (sLORETA), thus increasing the detection of localized neuronal activity (Grech et al., 2008; Pascual-Marqui, 1999; Pascual-Marqui, Esslen, Kochi, & Lehmann, 2002).

While studies have often used self-reported data, such as survey questionnaires, there are more advantages to using neuroimaging tools that could directly measure brain activity. Self-reported data is often limited by the participants' lack of knowledge or biases (Dimoka et al., 2011). For instance, an individual may fail to accurately answer psychometric measures in a given situation because he/she may be unaware of what drove he/she to specific decisions. However, directly measuring neural activity or physiological functions could produce more objective and generalized findings, thereby enhancing the information privacy field (Dimoka et al., 2011), particularly in providing a better understanding of the privacy paradox. Moreover, using a neuroimaging tool to measure brain activity allows for identifying the mental processes that are present when individuals make privacy-related decisions. These mental processes are distinct from beliefs, as they are spontaneous and less enduring, and maybe influenced by internal beliefs and external stimuli, as mentioned earlier (Angst & Agarwal, 2009; Dimoka 2012; Li et al., 2011).

4.3. Data Collection

The study was approved by the institutional review board (IRB) before any data was collected. IRB approval ensures that subjects are not mistreated, and data collected is handled carefully and safely so as to protect the subjects from any harm in the course of the study. To attain approval, the benefits and risks to participants, the method of data collection and data analysis, how the data is kept, as well as the overall importance of the study were documented. Appendix A contains the approval letter by IRB, indicating the study could proceed.

A within-subjects experiment (also called a repeated-measures experiment) is an experiment whereby each subject undergoes all the treatments (also called experimental conditions), with some control available to separate the effects of each treatment

(Dimoka, 2010; 2012). Essentially, each treatment consists of one or more of the independent variables, and usually at some level (Dimoka, 2012). For instance, the independent variable for a particular treatment, such as trust, is introduced at a high level and used to determine the subject's decision to disclose personal information. This same independent variable would then be introduced at a low level to measure subjects' decisions. Essentially, the independent variable is introduced at varying levels (such as high and low) to determine what effect it has on the dependent variable. Within-subject experiments reduce the number of participants necessary for adequate power, since all participants are exposed to all of the treatments, thus making it advantageous in reducing sample sizes and cutting costs for neuroimaging studies (Dimoka, 2012).

Studies in neuroscience sometimes have a small number of subjects, such as the study of Zotev et al. (2014) with six participants. Generally, however, the number of participants is often over twenty (Seeley, Smith, MacDonald, & Beninger, 2016; Xu, Shen, Chen, Ma, Sun, & Pan, 2011; Zotev, Yuan, Misaki, Phillips, Young, Feldner, & Bodurka, 2016). In this study, a total of twenty-seven subjects participated in the three experiments (where the three experiments were conducted as one experiment). Five of the subjects' data were used for analysis in a pilot study, which was used as feedback for improving on any drawbacks in the design of the experiment, as well as exploring drawbacks in the collection of continuous EEG data used for analysis. The data collected from the remaining twenty-two participants was used for analysis and testing the hypotheses. For the pilot study, three subjects were male, while two were female (n=5), while the main study consisted of eleven males and eleven females each (n=22), indicating an equal ratio of males to females.

As per IRB, participants were required to sign a consent form indicating they understood what was required of them in the study, the benefits and the risks, as well as their rights before beginning the experiments. Similarly, participants were required to sign a screening form indicating they were not pregnant, diagnosed with any psychological illnesses, or took any psychotropic medications. Pregnant women were excluded from the study so as to not induce any stress that could be caused when collecting data using an EEG, as well as to avoid any varied neuronal activity that may be caused by pregnancy. Brain activity in individuals who use psychotropic medications or suffer psychological illnesses may be different from individuals who do not use psychotropic medications or have psychological illnesses. This is evident, where theta brain waves can be moderated by dopamergic inputs in attention deficit hyperactivity disorder (ADHD) patients (di Michele, Prichep, John, & Chabot, 2005). Similarly, the use of psychotropic medications can induce specific hormonal changes to improve brain activity in specific areas (Demos, 2005).

4.3.1. Emotiv EPOC+ EEG

The experiments captured brain data using an EEG device known as the Emotiv EPOC+. The emotive EPOC+ is a 14-electrode commercial EEG device with two reference points. The fourteen electrodes corresponded to the following channels of the 10-20 system: AF3, F7, F3, FC5, T7, P7, O1, O2, P8, T8, FC6, F4, F8, AF4. The 10-20 system is an international standard used for EEG, which describes where electrodes should be placed (Teplan, 2002). Figure 7 depicts the emotive EPOC+ as well as the channel locations and their associated positions in the 10-20 system as detected by EEGLab.

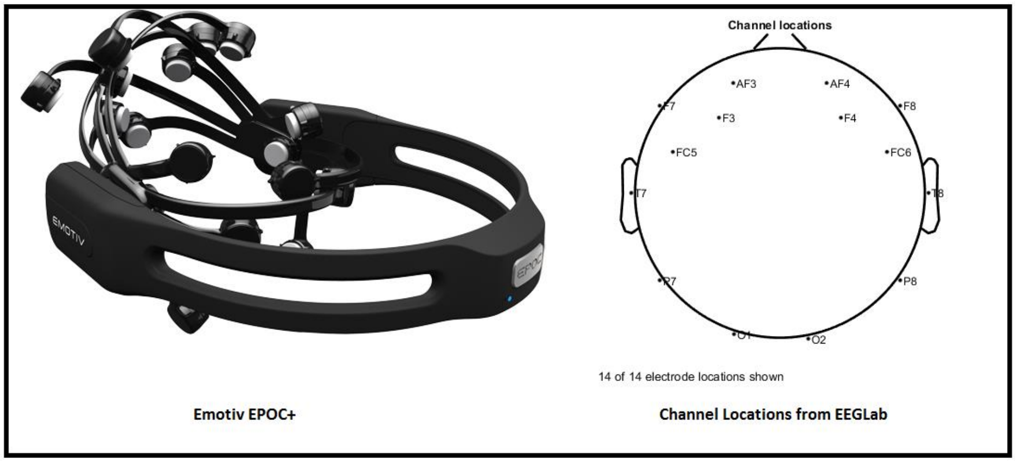


Figure 7. Emotiv Epoc+ Adapted from Emotiv Website and Channel Locations Depicted from EEGLab

4.4. Experiment Design

As explained above, the study is divided into three experiments, in which all subjects participated as if it were one experiment. Each experiment was designed as a within-subjects experiment. Experiment 1 was designed solely to capture the neural correlates of the independent variables of this study (i.e. privacy risk, trust, distrust, personal interest, and uncertainty). Experiment 2 was designed as a 2x2x2x2 factorial experiment whereby the independent variables of privacy risk, distrust, trust and personal interest were measured on two levels: high and low. Experiment 3 was designed as a 2x1 factorial experiment, where there were two levels of personal interest, and one level of uncertainty. Experiments 2 and 3 were designed for testing the relationships between the independent variables, privacy concerns and personal information disclosure.

Before subjects began the experiments, the emotiv EPOC+ EEG was fitted on their scalps according to the 10-20 system, and each electrode was tested to ensure electric potentials were captured for each channel. When all channels were responsive, subjects began the experiments, as if it were one experiment. During the experiments, subjects were allowed to take a break if they felt uncomfortable or stressed, at which point the emotiv EPOC+ was removed and recordings were stopped. When subjects were ready to resume, the emotiv EPOC+ was once again placed on the scalp, and all electrodes tested for data acquisition. In total, there were only two subjects who took a break. If at any point an electrode stopped collecting data or became faulty, the subjects were asked to stop and the electrode(s) was re-adjusted until data was once more captured. At times, this entailed an electrode moving out of position, bad connectivity using Bluetooth, or the electrode becoming dry.

Taken as one experiment, the least amount of time taken by one subject was fifteen minutes, while the longest was one hour and five minutes. However, every other subject took between thirty to forty-five minutes to complete the experiments. Overall, subjects were given the freedom to take as much time as they needed, so as to not apply any pressure on them. The times associated for when subjects were introduced to stimuli, and when they made their decisions were recorded for the creation of epochs for later analysis. When subjects completed the experiments, they were offered $50 as compensation for their participation.

4.4.1. Experiment 1: Neural Correlates

Experiment 1 consisted of five conditions/treatments, each pertaining to the mental processes identified in the external privacy calculus. Condition 1 pertains to privacy risk, condition 2 pertains to trust, condition 3 pertains to distrust, condition 4 pertains to uncertainty, and condition 5 pertains to personal interest. Conditions 1 to 4 utilized review profiles of simulated organizations and/or websites. Review profiles have been used in prior studies to elicit specific perceptions and observe subjects' decision-making (Ba & Pavlou, 2002; Dimoka, 2010). For example, Dimoka (2010) used feedback profiles to examine subjects' neural activity to the constructs of trust and distrust. In the context of ecommerce transactions, feedback profiles were found to be adequate treatments since they help buyers to accept or reject sellers (Pavlou & Dimoka, 2006). Similarly, the internet has been used by reviewers to provide useful feedback and reviews for organization and websites.

Conditions 1 to 3 reflected the factors of privacy risk, trust and distrust, respectively. Essentially, the profiles for conditions 1 and 3 consisted of negative reviews indicating the unsafe and opportunistic nature of the organization or website, while the profile for condition 2 consisted of positive reviews indicating the safety and benevolence of the organization or website. For the factor of uncertainty (condition 4), a similar review profile was used, but instead, there was very little and ambiguous information for the simulated organization or website. As explained above, uncertainty is related to ambiguity, but is often related to an assessment with doubtful outcomes (Pfeffer and Salancik, 1978). Alternatively, because of the ambiguous nature of a situation, uncertainty may not necessarily be considered as risk, but may influence risk (Krain et al., 2007). Condition 5, personal interest, was measured by allowing subjects to choose either an ecommerce product category that they would be highly interested in obtaining from online sellers, or an e-service which they may be more interested in using. Personal interest is the intrinsic motivation of the individual for the content requiring him/her to disclose his/her personal information (Dinev & Hart, 2006). Since peoples' personal interests are diverse, and they may decide to disclose their personal information for a variety of reasons such as convenience or the desire to obtain a specific item that can only be found online, an accurate means of measuring personal interest would be to actually let subjects choose something in which they have a vested interest. The profiles for experiment 1 are located in Appendix B.

For each profile (conditions 1-4), subjects were exposed to one review comment, and clicked the screen to move on to the subsequent comments, until all comments were read. All the previous comments were then aggregated on one screen, where questions were asked pertaining to their perception of the factor the treatment reflected, their privacy concerns for the organization or website they just read reviews for, as well as the likelihood that they would disclose their personal information to such organization or website. Specifically, subjects would be asked questions like "Do you believe it is a risk to disclose your personal information to LTPC?", "How concerned are you about the privacy of your personal information if you were to disclose it to LTPC?" and "Would you agree to disclose your personal information to LTPC?". Subjects answered each question on a seven-point Likert scale, ranging from 1 being the least likely to 7 being the most likely, which was used to stimulate brain activity regarding the treatment they were currently undergoing. This method of triggering brain activity has been used by Dimoka (2010), since the subjects would be processing the information about the organization or website they have just been exposed to (Dimoka, 2012). After answering all questions, subjects were then directed to a screen where they were asked to randomly click any number between 1 to 9. This acted as the control treatment to erase any perceptions from the treatment they had currently undergone, thus reducing any carryover effects. This method of control in a within-subjects experiment was used by Dimoka (2010), in her fMRI experiment of trust and distrust when buying online. Subjects iterated this process for conditions 1 to 4.

For condition 5, measuring the neural correlates of personal interest, subjects were exposed to a screen with a number of options from which to choose. After choosing a product category they were highly interested in obtaining online or an e-service (such as online banking, online education, e-health), subjects would click the screen to answer a similar set of questions as in the first four treatments. Since this study is not context-specific (i.e. ecommerce, ehealth), and is more concerned about individuals' decisions to disclose their personal information, the review profiles for simulated organizations or websites were altered to reflect the privacy practices of the organization or website.

It should be noted that the review profiles were developed to mimic feedback comments from Google Play, where users can rate an application on a five-point scale (represented as stars), and leave a comment about what they thought about the application. This is also similar to Amazon reviews. The mean score of users' ratings are then calculated to give the profile an overall score, and was also represented as a bar chart with a spectrum of colors (red means 1, green means 5) at the top of the profile. For this study, the profiles are all simulated, but developed to reflect the positive and negative comments that are associated with the variables of the study. For instance, a profile that reflected high trust would retain more review comments with 4-5 stars, and overall score closer to 5 (i.e. closer to 100% satisfaction), while a profile reflecting distrust would receive more 1-2 stars and an overall score closer to 1.

4.4.2. Experiment 2: 2x2x2x2 Factorial Experiment

Experiment 2 is a 2x2x2x2 within-subjects factorial experiment, whereby the independent variables of privacy risk, trust, distrust and personal interest each have two levels: high and low. The factorial experiment allows for studying both the main effects and the interaction effects of the independent variables against the dependent variables. Experiment 2 therefore had sixteen conditions in total, as seen in Table 3.

Table 3. 2x2x2x2 Factorial Design for Privacy Risk, Trust, and Distrust

Conditions	**Privacy Risk**	**Trust**	**Distrust**	**Personal Interest**
1	High	High	High	High
2	High	Low	High	High
3	High	Low	Low	High
4	Low	Low	Low	High
5	Low	Low	High	High
6	Low	High	High	High
7	Low	High	Low	High
8	High	High	Low	High
9	High	High	High	Low
10	High	Low	High	Low
11	High	Low	Low	Low
12	Low	Low	Low	Low
13	Low	Low	High	Low
14	Low	High	High	Low
15	Low	High	Low	Low
16	High	High	Low	Low

As stated earlier, experiments 1, 2 and 3 were designed as if subjects performed one experiment. This made it easier for them to complete each experiment without having to reschedule a meeting to do the other experiments. As such, the first eight conditions of the 2x2x2x2 factorial experiment followed on directly where experiment 1 ended. In so doing, the choice of product category obtained online or e-service subjects had the most interest in (condition 5 of experiment 1) was used as the means of manipulating the first eight conditions of experiment 2 for having a high level of personal interest. Subjects were asked to keep their choice in condition 5 of experiment 2 in mind, while proceeding to the next eight conditions, as if the website or organization offered the interested product category or service of choice.

Subjects were then exposed to the first eight conditions, each of which consisted of a review profile, similar to experiment 1. For each condition, subjects read one review comment before clicking to the subsequent review comments until they arrived at a screen where all comments were aggregated and questions were asked pertaining to their level of personal interest, risk, trust and distrust perceptions, as well as their privacy concerns and willingness to disclose their personal information to the organization or website. In essence, experiment 2 followed the same format as experiment 1, and the questions asked were similar, each of which was rated on a seven point Likert scale.

Review profiles were also designed similarly, as those in experiment 1. The review comments for each condition consisted of comments and aggregated scores to reflect the levels of each variable per condition. For instance, the profile that reflected high risk, high distrust, and low trust (conditions 2 and 10), had a lower mean score than the profile that had high risk, high distrust, and high trust (conditions 1 and 9), since the latter profile included a few positive comments reflecting trust. Alternatively, the profile that reflected high risk, low distrust and low trust (conditions 3 and 11) had a slightly higher mean score than the profile with high risk and high distrust, but low trust (conditions 2 and 10), since the former profile consisted of more negative comments.

Between each condition, subjects were asked to select a number between 1 and 9 before proceeding to the subsequent conditions. This acted as the control condition to reduce any carryover effects. When subjects completed the first eight conditions, they were presented with a similar screen as that of condition 5 from experiment 1, but instead of choosing a product category or e-service they were most interested in, they chose the one that they were least interested in. This acted as the manipulation for a low level of personal interest. Subjects then proceeded to complete the remaining conditions 9-16 in the same manner as they did for conditions 1-8. Conditions 9-16 utilized the same profiles as conditions 1-8, but under the condition that the subjects were looking at an organization or website for a product category they could obtain online or e-service in which they had little interest in.

4.4.3. Experiment 3: 2x1 Factorial Experiment

For uncertainty, a 2x1 within-subjects factorial experiment was designed. As mentioned above, uncertainty may consist of doubt for the outcome of a situation, but is differentiated from ambiguity in that it is more negative. As such, it was not included as a factor in experiment 2, since a review profile that contains comments over whether an organization or website is risky, or should be trusted or distrusted, should help better inform individual's decisions and would not be representative of uncertainty. However, uncertainty must be tested with personal interest to observe if there are any interaction effects. Specifically, while the research model in Chapter 3 did not hypothesize a significant relationship between personal interest and uncertainty, it is incumbent to test for any effects that may exist between the constructs when conducting an experiment. Therefore, a 2x1 factorial design (two levels for personal interest, one level for uncertainty) would be used.

The first condition of the 2x1 factorial experiment utilized the choice subjects made for condition 5 of experiment 1 to elicit a high level of personal interest. Subjects were asked to keep this choice in mind while reviewing the profile for the first condition of experiment 3. Similar to experiment 1 and 2, each comment was read by the subjects, then the screen was clicked to move on to the subsequent comments. When all the comments for the condition were read, they were aggregated and questions pertaining to the personal interest and uncertainty perceptions were asked, along with privacy concerns and willingness to disclose personal information. Each question was similar to those in experiments 1 and 2, and were all rated on a seven point Likert scale.

Subjects were asked to select a random number between 1 to 9 before moving on to the second condition of the experiment as the control condition to reduce any carryover effects. The second condition of the 2x1 factorial experiment utilized the choice subjects made for the least interested product category or e-service in experiment 2 in representing a low level of personal interest. Subjects then reviewed the profile and were asked to answer the same questions as in previous condition of this experiment.

4.4.4. Summary of Experiments

The study utilized three within-subjects experiments. However, all three experiments were conducted as if it were one experiment for the convenience of the subjects. Experiment 1 consisted of five conditions, used for assessing the neural correlates of privacy risk, trust, distrust, uncertainty and personal interest, respectively. Experiments 2 and 3 were factorial experiments, where experiment 2 consisted of sixteen conditions (2x2x2x2) and experiment 3 consisted of 2 conditions (2x1). In total, each subject underwent twenty-three conditions. A control condition was included to remove carryover effects between conditions, and entailed subjects randomly choosing a number between 1 to 9.

4.4.5. Validity Criteria

Experiments are used in social science research when the investigators want to observe a phenomenon, in a strictly controlled environment, where one or more variables are varied, but other variables are kept constant (Zimney, 1961). Essentially, the strict controlled environment in experimental research often sacrifices external validity for internal validity (Sekaran & Bougie, 2013). Specifically, in lab experiments, there is often a high level of internal validity, whereby researchers are able to make inferences over the causal relationships between independent and dependent variables, as opposed to the low level of external validity (Sekaren & Bougie, 2013). External validity refers to the generalizability of the results from an experiment to the field or organizational setting (Sekaren & Bougie, 2013). Essentially, the controlled environment of a lab experiment may not adequately represent the real world setting of a situation being examined, therefore sacrificing the external validity of the experiment. However, this tradeoff of external validity for strong internal validity is necessary in experimental research when the investigators wish to better understand a phenomenon, by examining the factors that influence the phenomenon (Sekaran & Bougie, 2013), such as in the case of this study, where a better understanding of the privacy paradox is the end-goal.

There are seven major threats to internal validity in any experiment, which are: history effects, maturation effects, testing effects, selection bias effects, mortality effects, statistical regression effects, and instrumentation effects (Sekaren & Bougie, 2013). History effects refers to unplanned effects on the dependent variable, when a relationship between in independent and dependent variable is being tested, that occur from extraneous variables that were not accounted for (Sekaren & Bougie, 2013). History effects were mitigated in experiments 1 to 3 due to the timeframe it took for each subject to complete the experiments, which lasted on average thirty to forty-five minutes, as discussed above. Additionally, each task in the experiments required the subjects to focus on the review profiles and answer specific questions (measurement items) based on what they read.

Maturation effects are similar in that there may be unplanned psychological changes over time on the subject that influences the relationship between the independent and dependent variable in an experiment (Sekaran & Bougie, 2013). The probability of a maturation effect in this experiment could have occurred because of its within-subjects design. However, this was mitigated through the control condition in place, where subjects chose a random number between conditions. Testing effects occur in situations whereby the subjects' responses are changed from the second administration of a test (Sekaran & Bougie, 2013). Testing effects usually occur when subjects are exposed to a pre-test (i.e. given a test to measure the dependent variable before being exposed to the treatment) and post-test (i.e. given a test to measure the dependent variable after being exposed to the treatment). A within-subjects experimental design with a proper control in place mitigates testing effects, such as in the case of this study.

Selection bias effects occur when the selection of participants do not match the criteria for the study (Sekaren & Bougie, 2013). An example of this would be selecting individuals who use psychotropic medications for the EEG experiment, which may affect their decision-making processes. However, a few criteria for subject participation was set to minimize selection bias, which mitigates the selection bias effects that may affect internal validity. Mortality effects refer to the attrition of members assigned to the different groups over the course of the experiment (Sekaren & Bougie, 2013). Specifically, over the course of the experiment, members of the various groups could drop out, which could affect the results of the experiment. Since this study utilized within-subjects experiments, there was no threat to internal validity from mortality effects, since there is essentially one group, where each subject is exposed to all the treatments.

Statistical regression effects occur when members chosen for a particular group has extreme scores on the dependent variable on the second administration of the test used to measure the dependent variable (Sekaran & Bougie, 2013). Random assignments of subjects to each group is a proposed means of addressing this issue, since it is most probable that subjects would be distributed between groups evenly. Statistical regression effects are even less of a problem in within-subjects designs, similar to mortality effects. Finally, the instrumentation effect occurs when the researcher makes changes as to what he/she wishes to observe during the course of the experiment (Cook & Campbell, 1979).

The use of a measurement item to assess the dependent variable, as well as the lack of a between-subjects experimental design helps in mitigating this threat.

4.5. Data Analysis

Before any data could be analyzed, data preprocessing of the raw EEG took place. Essentially, EEG data is collected in a continuous stream, and then chopped into a specific set of timeframes corresponding to key events (i.e. introduction to stimuli) known as epochs. These epochs are then used for analysis. Data is also cleaned to remove artifacts.

Since EEG captures a lot of data points, there are a number of techniques that can be used for analysis. One such method is the analysis of frequency bands (delta, theta, alpha, low beta, high beta, and gamma), which are compared against baseline brain activity (Massar et al., 2012; Schonwald & Muller, 2014). Frequency analysis is also quite common in neurofeedback research (Zotev et al., 2014; 2016). Alternatively, time-domain research of event related potentials (i.e. the brain activity after a subject is exposed to stimuli) analyzes the reflexive brain activity of subjects before conscious thought begins (Sur & Sinha, 2009). The P100, N100, P200, P300, mismatch negativity (MMN), and feedback related negativity (FRN) are some of the more popular components of event related potentials (ERPs) in EEG research (Massar et al., 2012; Sumich, Kumari, Heasman, Gordon, & Brammer, 2006; Sur & Sinha, 2009; Vance et al., 2014). Time-domain research has been used for a number of studies for assessing emotions and precognitive reactions of the brain (Olofsson, Nordin, Sequeira, & Polich, 2008). Massar et al. (2012) used time-domain research, specifically the effect of FRN in studying risk-taking behavior of individuals. In IS security research, Vance et al. (2014) measured the effect of the P300 in predicting individuals disregard of safety warnings.

EEG source analysis of event related potential constitutes another method of analysis, where the goal is to determine the localization of neuronal activity. While EEG has low spatial resolution, leading to the inverse problem, a number of techniques have been developed to estimate the dipoles of evoked potentials. The dipole is the flow of ions through the axons of neural tissue, whereby a scalp potential distribution map is generated based on the points within the cerebral cortex where estimated potential occurs (Scherg, 1990). Methods of dipole estimations fall into two categories: parametric and non-parametric. Dipole parameters are estimated based on a priori determined number of dipoles in parametric techniques, while non-parametric techniques estimate the dipoles' magnitude and orientation of at fixed positions in the brain volume. However, non-parametric techniques present a linear problem which are solved by different mathematical formulations (Grech et al., 2008).

Grech et al. (2008) reviewed a number of parametric and non-parametric techniques to solve the inverse problem, such as beamforming, BESA, MUSIC, FINES, simulated annealing and computational intelligence algorithms for parametric techniques. For non-parametric techniques, Grech et al. (2008) reviewed minimum norm estimates, (s)LORETA, variable resolution electrical tomography (VARETA), quadratic regularization and spatial regularization (S-MAP) using dipole intensity gradients, spatio-temporal regularization (ST-MAP), the Backus-Gilbert method, local autoregressive average (LAURA), shrinking LORETA FOCUS (SLF), standardized shrinking LORETA FOCUS (SSLOFO), and adaptive standardized LORETA FOCUS (ALF) for non-parametric methods. While different methods had their advantages with regards to specific constraints and parameters, LORETA was found to give satisfactory results, with sLORETA giving the best solution for localization (Grech et al. 2008). For this study, neural correlates of specific brain areas for mental processes were predicted to have an effect on privacy concerns and individuals' decisions to withhold or disclose their personal information. As such, sLORETA was the chosen method for analysis for all three experiments.

4.5.1. Preprocessing of Data

All EEG data were captured continuously with a sampling rate of 128Hz. Specifically, data are sampled 128 times per second, producing 128 timeframes per second. Key events were marked, when subjects were responding to the questions in each condition to be epoched for analysis (i.e. chopped into segments for analysis of key events). These questions were used to trigger brain activity as subjects were processing the stimuli with which they were presented (Dimoka, 2012). Continuous EEG files were exported from the emotiv PURE.EEG software in European data format (.edf) format, and converted using the PURE.EEG tool into comma separated value (.csv) files.

Data recorded on each channel were recorded as floating point values, where the direct current (DC) level of each signal occurred at approximately 4200 uV. Negative voltages were expressed as less than 4200, while positive voltages were expressed as more than 4200. Each .csv file was then cleaned as it contained information pertaining to timeframes per EEG, data captured by each electrode, contact quality, gyros, etc. Every additional piece of data other than the data captured by the fourteen channels were erased and saved as tab delimitated text files (.txt). Each file was then imported into EEGLab, a toolbox for Matlab for processing EEG data for removing the DC offset (i.e. changing the floating point values into root-mean squared (RMS) microvolts), removal of artifacts, and epoching.

Channel locations were first added to the imported data, where each channel's parameters were specified in the "channel locations" toolbox of eeglab. When the parameters were first entered, they were saved as a .ced file so that they could be imported for subsequent continuous EEG files. A high-pass band filter was applied with a lower tail frequency of 0.16. This changed the floating point values to RMS microvolts for analysis. Artifacts were removed manually, through each continuous EEG file. Artifacts are waveforms that are not of cerebral origin, and may consist of specific actions such as muscle movements and the blinking of eyes (Libenson, 2010). Artifacts can be gleaned based on wave morphology, such as in the case of eyeblinks, where a downward deflection of the waves occur (Libenson, 2010). There are numerous other artifacts such as eye movements, electrode pops, bad electrodes, among others. Usually, however, artifacts can be detected through distortion of waveforms in continuous EEG (Libenson, 2010). Figure 8 displays a snippet of artifact removal from one subject, where highlighted blue lines indicate selected waves as an artifact to be rejected. After the removal of artifacts, each file was epoched according to criteria described above, where 128 timeframes were extracted before subjects responded to questions (1000 milliseconds). A similar method of epoching based on subjects answering questions was done by Cannon (2009).

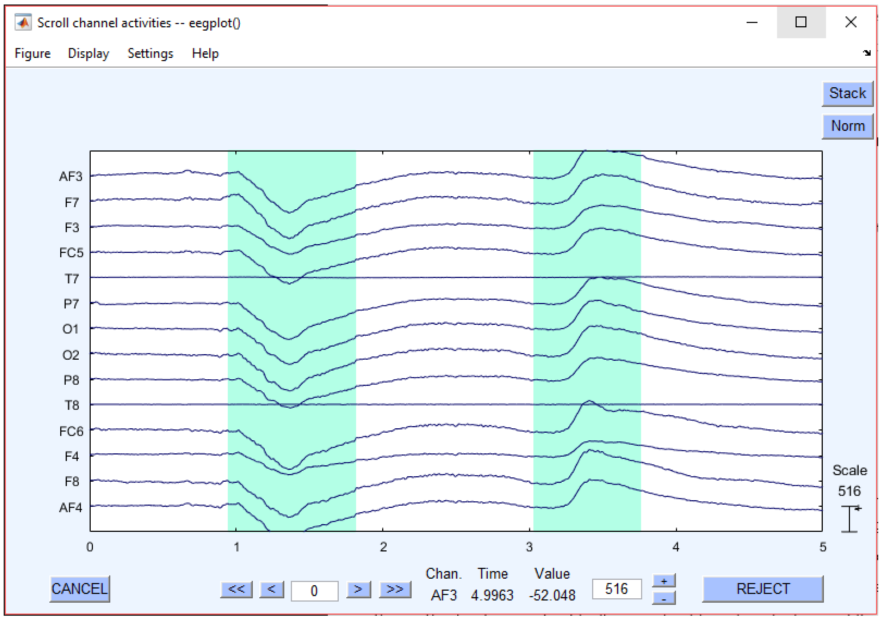


Figure 8. Artifact Removal in EEGLab

4.5.2. Transformation into sLORETA Images.

After preprocessing and epoching the data, all files (stored as tab delimitated text files) were sent to sLORETA for transformation into sLORETA images. This required the creation of an electrode coordinate text file, with all channels corresponding to the order in which data values per channel were recorded (i.e. AF3 recorded data in the first column of all data files, and was therefore the first electrode specified in the electrode coordinate file). The sLORETA utility was used to create an .sxyz electrode coordinate file, which was then used to create the transformation matrix required for performing the computational analysis of localized brain areas. Using the transformation matrix, all epoched data files were transformed into .slor files which produced sLORETA images, current source density and localization for each timeframe per file, per subject.

LORETA calculates the volume elements (voxels) of the cortical gray matter (Pascual-Marqui et al., 2002). LORETA uses realistic electrode coordinates for a three-concentric shell spherical head model co-registered on a standardized MRI atlas with talairach coordinates (Cannon, 2012). Talairach coordinates system is a 3-dimensional atlas of the human brain, that maps locations of brain structures from individual differences in the size and shapes of the brain (Talairach, 1998). It consists of three axes, the x-axis which corresponds to the left and right sides of the brain, y-axis which corresponds to the posterior and anterior locations of the brain, and z-axis corresponding to the dorsal (upwards) and ventral (downwards) positions of the brain. Current source density is mapped to 2,394 voxels of $7mm^3$ dimensions, with a maximum error of 14mm (Pascual-Marqui, 1999). The improved version of LORETA, the sLORETA, which was used for this study, utilizes the MRI atlas from the Montreal Neurological Institute (MNI), an alternative to the Talairach atlas, which consists of 6,329 voxels of $5mm^3$ (Cannon, 2012). In comparison to the 1mm resolution of fMRI and PET (Huettel & Song, 2008), sLORETA is proposed as an adequate solution to the inverse problem, whereby Pascual-Marqui (2002) argued that localization error cannot be improved beyond sLORETA.

4.5.3. Data Analysis for Experiment 1

Single group zero-mean t-tests were used by Pascual-Marqui et al. (2002) to compare three methods of source localization in an experiment where seventeen subjects were exposed to neutral facial affect. Hotspots (i.e. areas of brain activity) were captured and compared between each technique, where all brain areas had an equal probability of containing a hotspot (Pascual-Marqui et al., 2002). Specifically, there was no favored brain area, and the experiment was used to determine where statistically significant brain activity occurred in the seventeen subjects. Similarly, single group zero-mean t-tests utilizing Statistical non-Parametric Mapping (SnPM) were used for each of the conditions of experiment 1. Essentially, the group means of brain activity were compared against a group with brain activity of zero-mean.

EEG data transformed to sLORETA images produce localized brain activity for every timeframe. SnPM allows for testing the timeframe of interest where statistical significance is met, and the location of brain activity for this timeframe is determined (Pascual-Marqui et al., 2002). Specifically, t-tests are produced for every timeframe for each subject, whereby three numbers corresponding to MNI coordinates (X, Y, and Z axes) are multiplied by the total number of voxels (i.e. 3x6329), resulting in 18,987 variables (Pascual-Marqui et al., 2002). For each subject, the total number of variables are multiplied by the timeframes (i.e. given 128 timeframes, 18,987x128), resulting in 2,430,336 t-tests. Pascual-Marqui et al. (2002) argued that the univariate t-distribution cannot determine statistical significance for testing brain activity, as multiple comparisons of nearly one million variables (in this case, based on the data produced from the experiments and the use of sLORETA, nearly 2.5 million variables), do not correspond to a univariate t-distribution, nor is the t-statistic representative of the Student's t-test if current source density does not have a normal Gaussian distribution. Thus, SnPM solves statistical errors used for testing neural activity by estimating the probability distribution through the randomization procedure, while retaining the highest possible statistical power (Pascual-Marqui et al., 2002).

For each condition, all subjects per condition were tested using SnPM, where threshold t-values at significance levels of 0.01, 0.05, and 0.10 for two-tailed and one-tailed tests were produced, as well as t-statistics for each timeframe. This was done by first analyzing the raw EEG data from epoched files per condition. Threshold t-values and t-statistics for each timeframe were determined through randomization tests of 5000 (Nichols & Holmes, 2001). Timeframes with a t-statistic meeting or surpassing the threshold values at $p \leq 0.05$ were group-transformed into sLORETA images for the brain area where localization occurred using the .slor files produced for each subject, for each condition.

4.5.4. Data Analysis for Experiments 2 & 3.

Data analysis techniques were the same for experiments 2 and 3. Firstly, for experiment 2, region of interest (ROI) seed files were created using sLORETA utility for all sixteen conditions, where each ROI seed pertained to the neural correlates of brain activity for the conditions 1, 2, 3 and 5 of experiment 1 (condition 4 pertained to uncertainty, which was excluded from experiment 2), as can be seen in Appendix C. The ROI seed file was then used to extract the log of current source density values for every timeframe in the .slor epoched files of conditions 1-16 in experiment 2. This resulted in a text file of the log transformation of CSDs for each ROI specified and one single voxel (its nearest neighbor), for each subject for each condition in experiment 2. Log transformation of data is one technique of many data transformation techniques that are used to simplify complex data, as well as provide normality to otherwise non-normal data (Osbourne, 2002). As violations of normality could hinder certain parametric tests, data transformations are often used in fields such as social sciences (education, psychology) and biology, where normality is rare (Micceri, 1999; Osbourne, 2010).

ROI analysis has been used in fMRI research (Poldrack, 2006), and was used by Dimoka (2010) to determine the effect neural correlates of trust and distrust had in predicting price premiums. Additionally, Dimoka (2010) then developed a regression model with independent variables based on ROI values to predict price premiums. Following such method of analysis, the average log CSD per ROI was extracted for each subject in each condition of experiment 2, and placed in a regression model denoted by

$$y = \beta_0 + \beta_1 \ + \ \beta_2 + \cdots + \ \beta_j + \ \varepsilon \qquad (1)$$

where:

y is the dependent variable,

x is the dependent variable,

β_0 is the value of y when each value of x = 0,

β_j is the value of y based on unit change of x_j

as independent variables against the dependent variable of privacy concerns. This was done to test the hypotheses related to the neural correlates of the mental processes of the extended privacy calculus model (see Chapter 3), and privacy concerns. A second regression model was developed using the average log CSD per ROI of brain areas for the neural correlates of risk (independent variables) and trust (dependent variables). A third regression model was developed where the average log CSD per ROI per subject in each condition, and the response of each subject in each condition for privacy concerns were regressed against their willingness to disclose their personal information.

The regression models produced unstandardized beta coefficients of each independent variable ($\beta_j x_j$) which represented the amount of change in the dependent variable based on one unit change in the independent variable, *y* (Sekaran & Bougie, 2013). Positive beta coefficients represent an increase in *y* when x_j increases by one unit, while a negative beta coefficient represents a decrease in *y* when x_j increases by one unit. Similarly, for each beta coefficient, standardized beta coefficients were produced, whereby the beta coefficients are standardized to a mean of zero and a standard deviation of one (Sekaran & Bougie, 2013). The t-statistic and p-values were used to determine the significance of the relationships between the independent variables and dependent variables. Together with the sign (positive or negative) of the beta coefficients, as well as the significance of the relationships between independent and dependent variables, the hypotheses 6 to 11 (both experiment 2 and 3) were rejected or accepted for main effects. All analysis was done using SPSS. Interaction effects (hypothesis 12) were tested using R, where the same statistics were used to test the relationships of the interactions (i.e. beta coefficients to determine the effect, and t-value and p-value to determine the significance).

The regression models produced a coefficient of determination called the R-squared value denoted by,

$$R^2 = 1 - \frac{SS_E}{SS_T} \tag{2}$$

where SS_E is the error sum of squares (the degree to which the data points vary when compared to the estimated regression line), and SS_T is the total sum of squares (the degree to which data points vary when compared to their mean). The coefficient of determination explains the extent to which the variation in the independent variables vary from the dependent variables (Sekaran & Bougie, 2013). The adjusted R-square value was also calculated, denoted by

$$R_{adjusted} = 1 - \frac{(1 - R^2)(n-1)}{(n-p-1)} \tag{3}$$

where,

n is total sample size,

p is the number of predictors

The adjusted R-square adjusts the R-square statistic based on the number of independent variables in the model.

An Analysis of Variance (ANOVA) test was produced for each regression model to explain how well the independent variables explain the dependent variables with an F-statistic denoted by

$$F = \frac{Between\!-\!group\ variability}{Within\!-\!group\ variability} \tag{4}$$

where an F-value significant at $p \leq 0.05$ indicates the model's independent variables are a better predictor of the dependent variables as opposed to the constant-only (i.e. β_0) model. Finally, the tolerance (equation 5) and variance inflation factors (VIF, denoted in equation 6) were used to test for multicollinearity of the independent variables where

$$T = 1 - R_i^2 \tag{5}$$

$$VIF = 1/(1 - R_i^2) \tag{6}$$

where,

R_i^2 relates proportion of variance in the *i*th independent variable that is not related to other independent variables in the model (O'Brien, 2007). Several "rules-of-thumb" are given concerning the tolerance and VIF values for detecting multicollinearity. The higher the tolerance value (i.e. the closer to 1) the less likely multicollinearity exists, while a lower VIF indicates lower multicollinearity. While some researchers use a tolerance value as high as 0.70 to indicate multicollinearity (Dimoka, 2010), values as low as 0.10 are accepted, while VIF values as high as 10 and lower are considered acceptable (O'Brien, 2007).

Experiment 3 followed the same type of analysis as experiment 2. An ROI seed file was created using the sLORETA utility for brain areas associated personal interest and uncertainty identified in experiment 1 (conditions 4 and 5). The ROI seed file was then used to extract log CSD of each subject in each condition of experiment 3 for each ROI, from the .slor epoched files for experiment 3. The log CSD of each ROI was produced, whereby the average log CSD per ROI was input into a regression model as independent variables against the dependent variable of privacy concerns. The second regression model was developed using the average log CSD per ROI and privacy concerns as independent variables and subjects' willingness to disclose their personal information as the dependent variable. The statistics used for testing the hypotheses and model fits were the same as described for experiment 2.

4.5.5. Summary of Data Analysis for all Experiments and Hypotheses Testing.

Hypotheses 1 to 5 were developed to determine the neural correlates of privacy risk, trust, distrust, uncertainty and personal interest, respectively, in experiment 1. Data analysis was carried out on the epoched text files containing data collected by each electrode for each subject per condition using paired groups zero-mean SnPM t-tests. Essentially, the timeframes per subject per condition were compared, where threshold t-distributions were produced to determine which timeframes were statistically significant. The .slor transformed files were then analyzed as a group, where the statistically significant timeframe(s) indicated the localized source of brain activity.

Hypotheses 6 to 9 and hypothesis 11 corresponded to experiment 2. These hypotheses were tested by producing an ROI seed file using sLORETA for all the brain areas identified in conditions 1-3, and 5 of experiment 1. The ROI seed file was then used to extract the log transformation of CSD of each ROI per subject per condition, and its nearest neighbor voxel. The average log CSD per subject per condition per ROI was used as independent variables in a regression model against the dependent variable of privacy concerns. A second regression model was developed to test the relationship between the neural correlates of trust and risk, using the average CSD of the ROI of the neural correlates for trust and risk identified in experiment 1. The third regression model tested the relationship of the log CSD of each ROI and privacy concerns as independent variables, against the dependent variable of personal information disclosure.

Hypotheses 10 and 11 corresponded to experiment 3, where an ROI seed file was produced for the brain areas identified in conditions 4 and 5 for experiment 1 were produced. Similar to experiment 2, the ROI seed file was used to extract the log transformation of CSD for each ROI for each subject in each condition. The average log CSD was used as independent variables for a regression model against privacy concerns, and a second regression model where privacy concerns were also an independent variable was used against the dependent variable of personal information disclosure.

4.6. Summary

Three within-subjects lab experiments using an EEG were conducted to collect data and test the hypotheses of this study. However, subjects performed all three experiments as if they were one. Experiment 1 consisted of five conditions, used for capturing the neural correlates of privacy risk, trust, distrust, uncertainty and personal interest. Experiment 2 was a 2x2x2x2 factorial experiment, whereby personal interest, privacy risk, trust and distrust were all varied on two levels. Experiment 3 was a 2x1 factorial experiment where personal interest varied on two levels, but uncertainty remained at only one level. Review profiles were used for simulated organizations and/or websites as manipulations for the various conditions in the experiments. However, personal interest was manipulated by asking subjects to choose a product category or service they were interest in, using ICTs.

Neural correlates were derived using sLORETA, a mathematical formulation for identifying the localization of brain activity. SnPM t-tests of zero-means were used to analyze the neural correlates in experiment 1. Regression models were developed for experiments 2 and 3, where log-transformed CSDs of ROIs of brain areas identified in experiment 1 were used as independent variables, while privacy concerns were used as a dependent variable for the first model, and an independent variable in the second model, for each experiment.

Chapter 5

Results

5.1. Introduction

This chapter presents the results of the experiments used to test the research model and hypotheses. Section 5.2 describes the outcome of the pilot study, while section 5.3 contains the results of experiment 1. Sections 5.4 and 5.5 present the results for experiment 2 and 3 respectively. Section 5.6 contains the summary, included in which, highlights the hypotheses that were rejected and supported.

5.2. Pilot Study

Five subjects were used for the pilot study, whereby three were males and two were females. The primary objective of the pilot study was not used for acquiring neural correlates, as the sample size was too low for any significant results, nor for examining relationships between variables used for the regression models in experiment 2 and 3. The pilot study was first used to identify limitations in the experiments themselves (i.e. flaws in presenting the stimuli to subjects, and marking the key timeframes to which events took place). The pilot allowed for making adjustments to the questions which at first may have been difficult for subjects to interpret. Data acquired from the pilot study was preprocessed, epoched and transformed into sLORETA images. SnPM was used on the pilot data for each of the experiments, but there were no significant timeframes.

However, the pilot study did provide some insights for the analysis of the actual experiments. Firstly, instead of log-transformed CSD for each ROI, the pilot study initially used the actual CSD values. However, this led to a lot of outliers, skewed datasets, and non-normal distributions. Moreover, when actual CSD values were not computed well in the regression models, which led to almost all variables being removed. Utilizing the log-transformation of the pilot data corrected many of these errors and led to better model fits indicating that log-transformations should be used for the actual experiments. Analysis of the pilot data also led to extracting the CSD for a single voxel and its nearest neighbor for ROIs, rather than selecting all the voxels associated with one ROI. Essentially, the CSD of all voxels for a specific ROI produces results that are often inaccurate with very high multicollinearity.

5.3. Experiment 1: Neural Correlates

Zero-mean t-tests were used to acquire significant neural correlates for the mental processes that predict privacy concerns and personal information disclosure in the extended privacy calculus model. SnPM was used with a randomization of 5000 to establish threshold t-distributions for each condition, where timeframe(s) that surpassed the threshold t-value at $p \leq 0.05$ were significant. Group analysis of significant timeframes then revealed the location of neural correlates associated with mental processes for privacy risk, trust, distrust, uncertainty and personal interest.

5.3.1. Neural Correlates for Privacy Risk

For privacy risk (condition 1), threshold values were calculated by sLORETA SnPM, where significant t-values for one-tailed t-tests were 4.014 and -3.994, and 4.3 for two-tailed tests at a p-value of 0.05. There was significant activation in the right BA 32

(MNI coordinates: 10, 35, 20), which is part of the right anterior cingulate cortex in the limbic lobe (t-value: -5.67, $p < 0.01$). Additionally, there was significant activity in the left BA 9, the medial frontal gyrus, which is part of the frontal lobe (MNI coordinates: -5, 55, 20; t-value: -4.30, $p < 0.05$). While brain activity in the insular cortex (BA 13) was produced, the t-values were below the threshold levels and thus insignificant. Figure 9 depicts the significant brain activity for risk perceptions in privacy-related situations. Significant brain activity is shown in bright yellow, at 0 mm, where LORETA values were at their highest (LORETA values are in the square brackets after the [X, Y, Z] MNI coordinates at the top of each image).

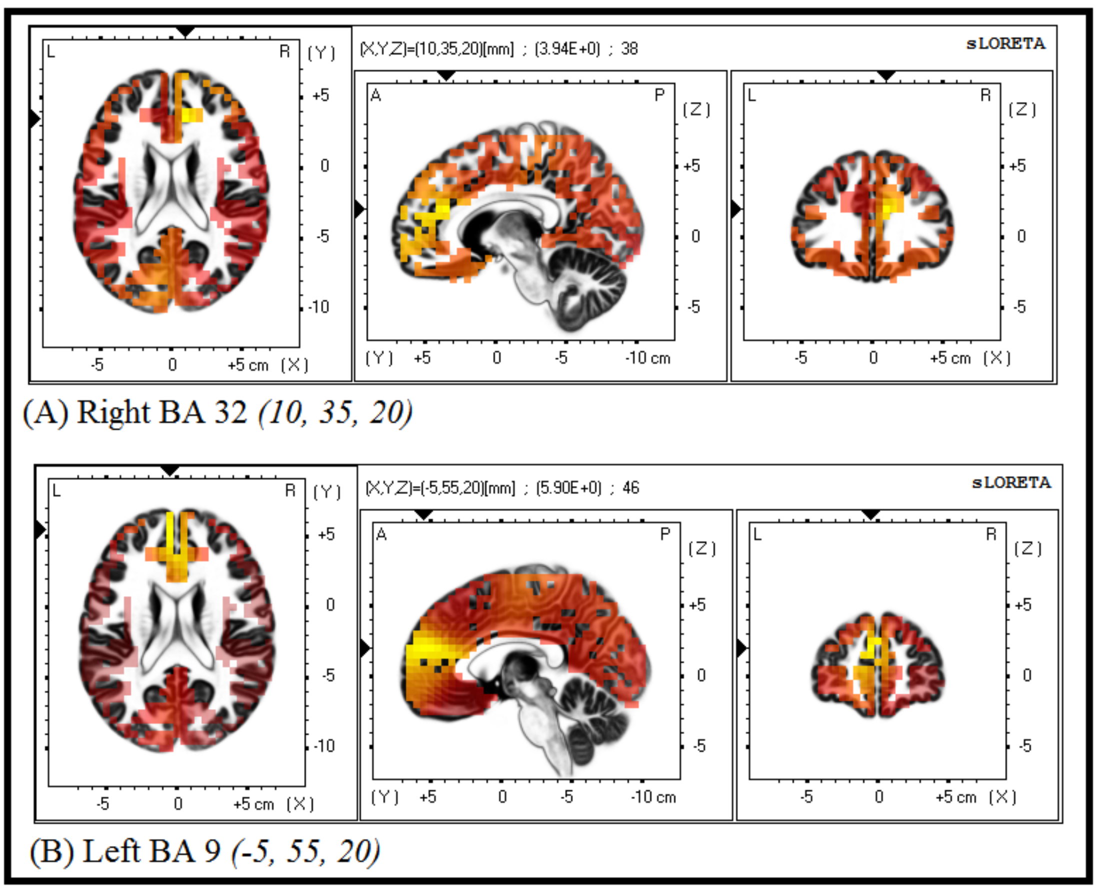


Figure 9. Neural Correlates of Risk Perceptions. Significant activity in yellow; A (BA 32) and B (BA 9) at 0mm. Brain slices from left to right depicting horizontal, sagittal and coronal planes.

To check for activation in the nucleus accumbens, the methodology developed by Lacadie, Fulbright, Constable, and Papadematris (2008) was used to determine the MNI coordinates for brain areas. This methodology was proposed by Lacadie et al (2008) as a better and more accurate means of determining functional neuroanatomical regions since it compensates for the actual differences between MNI templates and the Talairach atlas. The MNI coordinates for the right nucleus accumbens are (10, 10, -12), while the left nucleus accumbens has the coordinates (-11, 9, -11). However, there were no significant activations at these MNI coordinates. The results rejects hypotheses 1a and 1b, but supports hypothesis 1c.

5.3.2. Neural Correlates of Trust

Threshold values for condition 2, trust perceptions, for a zero-mean t-test were calculated where t-values at 4.082 and -4.121 were significant at p-value 0.05 for one-tailed tests, and 4.367 for a two-tailed test. There was significant activation of brain activity in the right BA 47, which is part of the inferior frontal gyrus in the frontal lobe (MNI coordinates: 15, 20, -15; t-value: 6.13, $p < 0.01$ at a two-tailed level). While MNI coordinates (15, 20, -15) are considered to be BA 47 based on sLORETA, the methodology by Lacadie et al. (2008) designates these coordinates as BA 11. Both BA 47 and BA 11 are considered as part of the orbitofrontal pre-frontal cortex along with BA 10 (Kringelbach, 2005). Dimoka (2010) found that the caudate nucleus and putamen were activated in trusting situations. To test if these areas had any significant activations, the MNI coordinates of the caudate nucleus (right: 13, 13, 11, left: -11, 13, 10), and putamen (right: 25, 3 -1, left: -26, 0, 2), were derived based on the methodology of Lacadie et al.

(2008). However, there were no activity at any of these MNI coordinates. Figure 10 depicts the brain activity related to trust perceptions in privacy-related situations. Based on these results, neither hypothesis 2a nor 2b are supported. However, the test did reveal right BA 47 as the source of localization for trust perceptions.

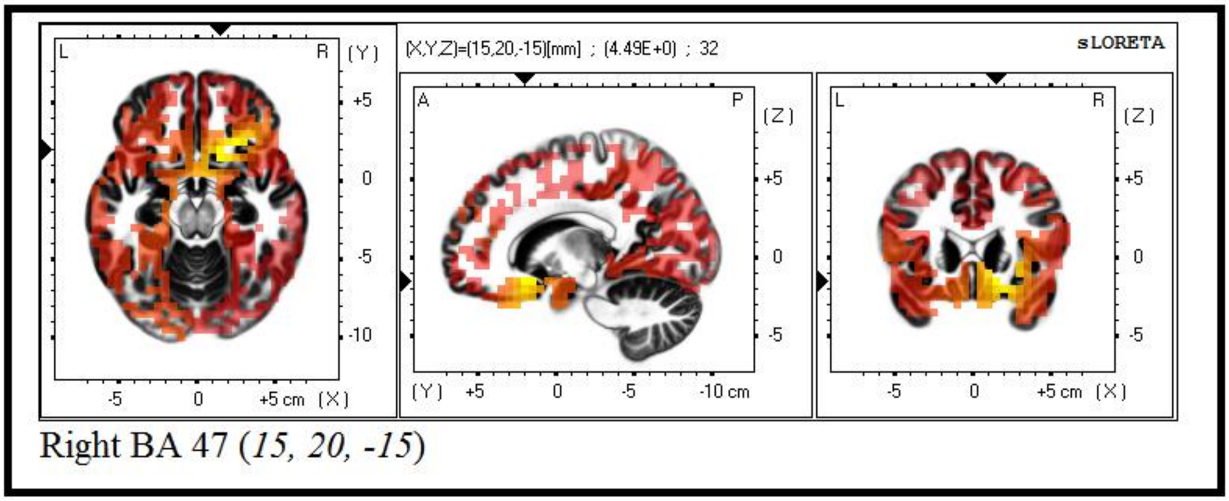


Figure 10. Neural Correlates of Trust Perceptions. Significant activity in yellow; BA 47 at 0mm. Brain slices from left to right depicting horizontal, sagittal and coronal planes.

5.3.3. Neural Correlates of Distrust

Threshold values for condition 3 (distrust) were calculated by sLORETA SnPM, where t-values of 4.290 and -4.254 were significant at p-value 0.05 for one-tailed tests, and 4.548 was significant at p-value 0.05 for a two-tailed test. Significant activity was found in the right BA 31 (MNI coordinates: 15, -25, 45; t-value: -4.41, $p < 0.05$), which is a part of the posterior cingulate gyrus, in the limbic lobe. There was also brain activity in the right BA 13 (MNI coordinates: 35, -5, 20; t-value: -4.29, $p < 0.05$), which constitutes part of the right insula cortex. Neural correlates for distrust are depicted in Figure 11. The methodology developed by Lacadie et al. (2008) gives the amygdala the MNI coordinates (right: 21, -1, -22 and left: -24, 0, -21). However, there was no activity at either right or left MNI coordinates of the amygdala at significant timeframes.

Hypothesis 3a was not supported, but the source localization for distrust occurred in the right BA 31, and right BA 13, the insula cortex, indicating hypothesis 3b was supported.

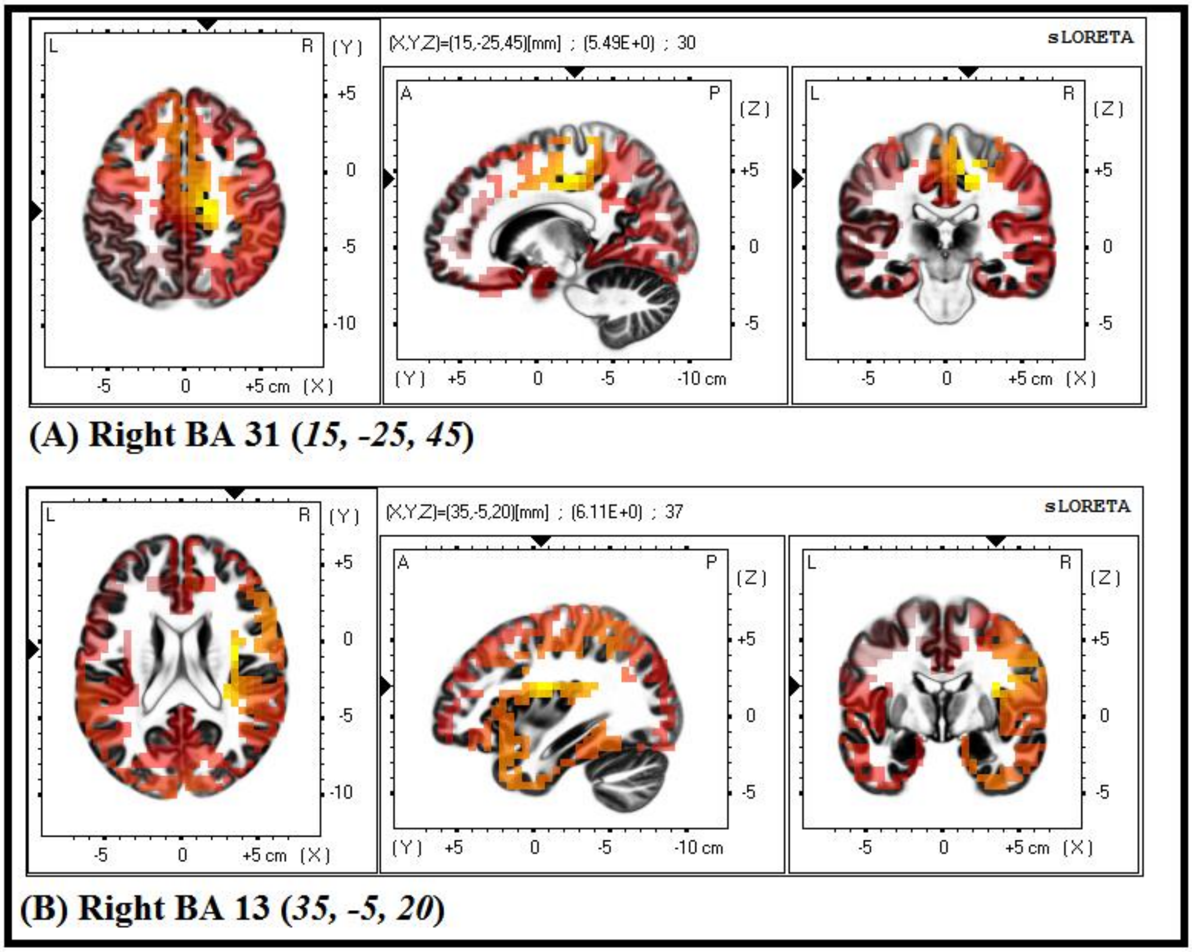


Figure 11. Neural Correlates of Distrust Perceptions. Significant activity in yellow; A (BA 31) and B (BA 13) at 0mm . Brain slices from left to right depicting horizontal, sagittal and coronal planes.

5.3.4. Neural Correlates of Uncertainty

Neural correlates were assessed in condition 4, where threshold values were calculated using sLORETA SnPM. T-values at 4.307 or -4.317 were significant at p-value 0.05 for one-tailed tests, while a two-tailed test required a t-value of 4.636 for a p-value of 0.05. There was significant brain activity in the right BA 40 (MNI coordinates: 50, -50, 55; t-value: -4.441, $p < 0.05$). BA 40 is a part of the inferior parietal lobule in the parietal lobe. There was also significant activation in the right BA 47 the inferior frontal gyrus in the frontal lobe (MNI coordinates: 45, 30, -5, t-value: -4.663, $p < 0.05$). BA 47 is a part of the orbitofrontal prefrontal cortex, along with BA 10 and BA 11 (Kringelbach, 2005). Thus, hypotheses 4a and 4b were supported. Figure 12 illustrates the localization of neural correlates for uncertainty perceptions.

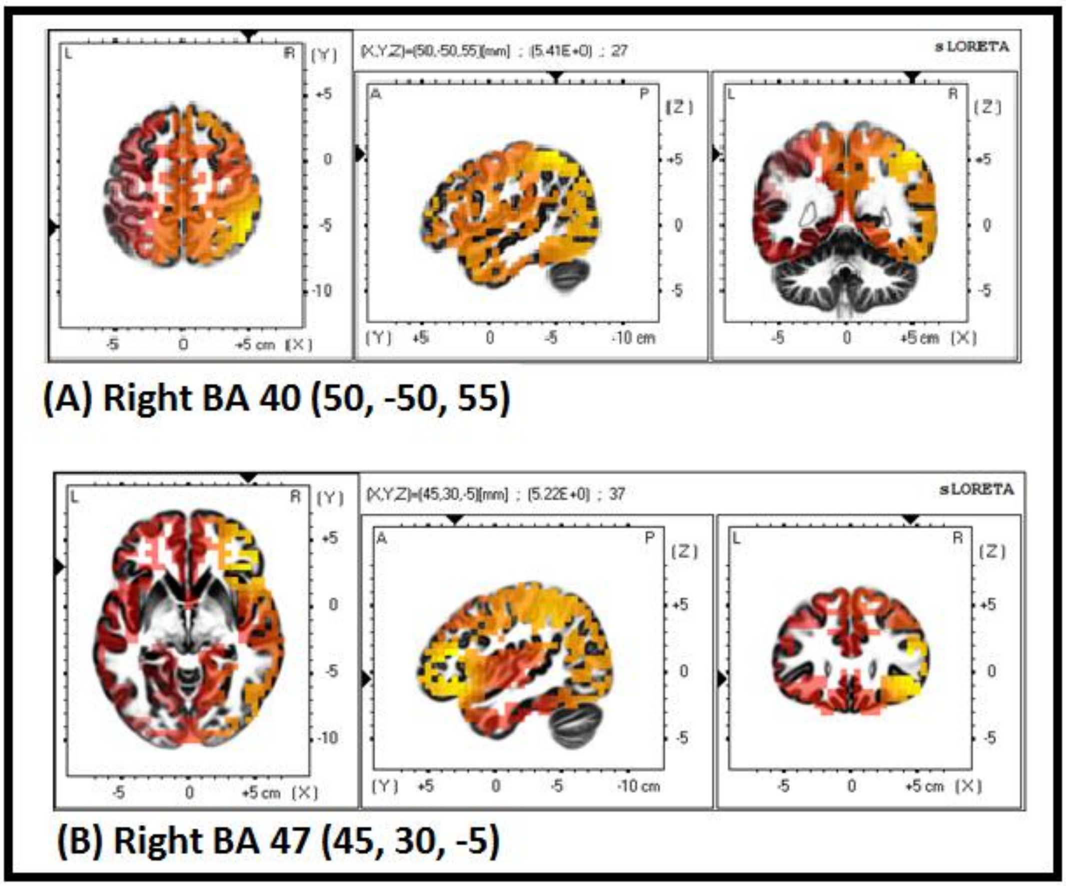


Figure 12. Neural Correlates of Uncertainty Perceptions. Significant activity in yellow; A 40 and BA 47 at 0mm. Brain slices from left to right depicting horizontal, sagittal and coronal planes.

5.3.5. Neural Correlates for Personal Interest

Threshold t-values were calculated for zero-mean t-tests for condition 5 (personal interest). For one-tailed tests, t-values at 4.077 and -4.099 were significant at p-value 0.05, while a t-value of 4.393 is significant at p-value 0.05 for two tailed tests. There was significant activation in left BA 40, inferior parietal lobule (MNI coordinates: -40, -50, 60; t-value: -4.20; $p < 0.05$), and left BA 37, middle temporal gyrus in the temporal lobe (MNI coordinates: -60, -65, 5; t-value: -4.34, $p < 0.05$). Thus, hypothesis 5a was not supported; however, hypothesis 5b was supported and localization for personal interest was inferred to be correlated with neuronal activity at left BA's 40 and 37. Figure 13 depicts the brain activity for subjects choosing an e-service or product they are personally interested in obtaining online.

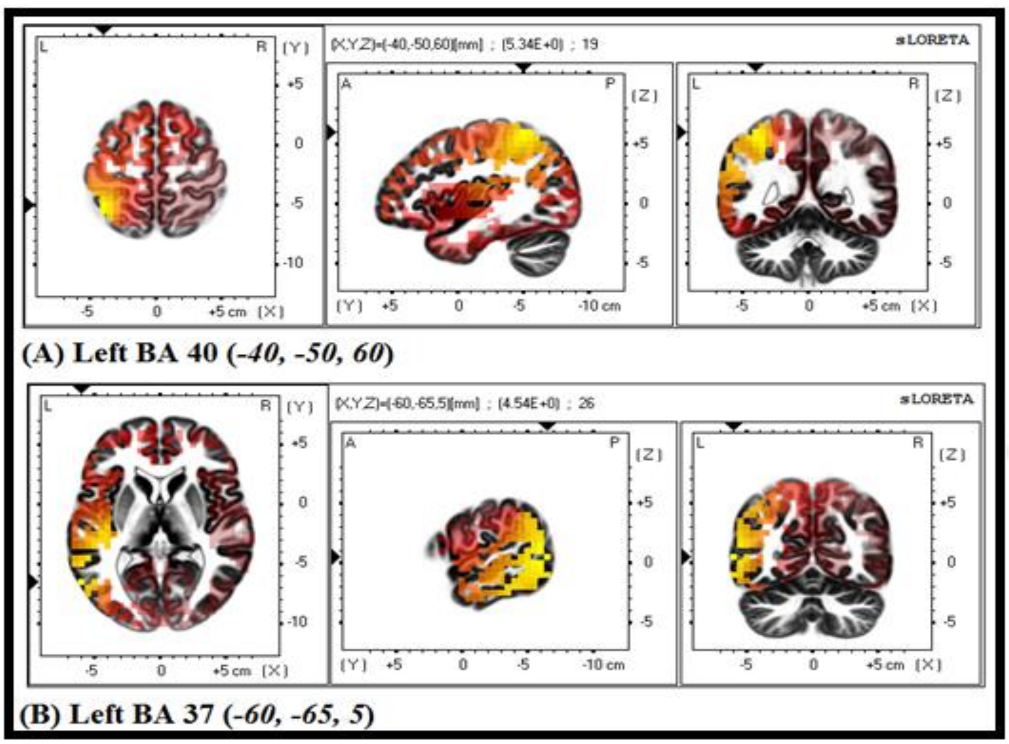


Figure 13. Neural Correlates for Personal Interest. Significant activity in yellow; A (BA 40), and B (BA 37) at 0mm. Brain slices from left to right depicting horizontal, sagittal and coronal planes.

5.4. Experiment 2: 2x2x2x2 Factorial Experiment

Using sLORETA, a seed file with the ROIs of BAs based on experiment 1 for neural correlates of personal interest, risk, trust and distrust was created. This seed file was used to extract the log-transformed CSD values for each ROI voxel and its nearest neighbor, for each subject for each of the sixteen conditions. The average log CSD per ROI was then plugged into a regression model to determine the effect of each neural correlate in influencing privacy concerns and in a second model to determine the influence of each neural correlate in influencing personal information disclosure. Table 4 shows the descriptive statistics for the variables of the sixteen conditions.

Table 4. Descriptive Statistics for Experiment 2

Variables	Mean	Standard Deviation
Right BA32	5.21	1.19
Left BA 9	5.68	1.17
Right BA 47	5.98	1.10
Right BA 31	4.45	1.21
Right BA 13	5.49	1.17
Left BA 40	4.99	1.17
Left BA 37	5.32	1.04
Privacy Concerns	5.48	1.58
Personal Information Disclosure	3.03	1.92

5.4.1. Regression Model for Privacy Concerns

Using SPSS and R, a regression model was developed to determine the change in the dependent variable of privacy concerns due to the influence of the independent variables of Right BA32, Left BA9, Right BA47, Right BA31, Right BA13, Left BA40, and Left BA37. The model had an R-square value of 0.055 ($R^2 = 0.055$), while the adjusted R-square value was 0.036. This indicated that the variance predicted by the independent variables was poor. However, the model had an F-value of 2.852 at p =

0.007, indicating its significance in predicting the dependent variable, privacy concerns, with the independent variable. Table 5 presents regression coefficients for the dependent variable privacy concerns.

Table 5. Regression Model for Dependent Variable: Privacy Concerns

Independ-ent Variables	**Beta Coeffici-ent**	**Standardiz-ed Beta Coefficient**	**Significan-ce (t-value)**	**Signific-ance (p-value)**	**Toleran-ce**	**VIF**
Right BA32	0.421	0.317	1.654	0.099	0.075	13.4
Left BA9	-0.075	-0.055	-0.405	0.686	0.147	6.78
Right BA47	0.355	0.247	1.853	0.065	0.154	6.48
Right BA31	0.029	0.022	0.143	0.887	0.113	8.85
Right BA13	-0.396	-0.294	-2.199	0.029*	0.153	6.52
Left BA40	-0.116	-0.086	-0.752	0.452	0.210	4.77
Left BA37	-0.025	-0.016	-0.232	0.816	0.561	1.78

* $p \leq 0.05$, ** $p \leq 0.01$, *** $p \leq 0.001$

The results of Table 5 indicated that only right BA 13 is significantly related to privacy concerns. All other variables are above the threshold 0.05 p-value. However, BA 13 has a standardized beta coefficient of -0.294, indicating a negative relationship with privacy concerns. Essentially, higher neural activity in BA 13 is related to lower privacy concerns. This result is opposite to hypothesis 8a. Thus, while the relationship is significant, the hypothesized direction of the relationship is not supported. Similarly, hypothesis 6a was not supported since the relationships are not significant. There were also no significant relationships when checking the interaction effects of the independent variables on the privacy concern. Thus, hypothesis 12a was rejected.

5.4.2. Regression model to Determine the Relationship between Risk and Trust

The neural correlates of risk (right BA 32 and left BA 9) were regressed against the dependent variable of trust (right BA 47). The regression model contained an R-squared value of 0.799 and an adjusted R-squared value of 0.798, indicating a high power in explaining the variance of the dependent variable with the variance of the independent variables. The model produced an F-value of 693.95 at $p < 0.001$. This indicated the independent variables were better predictors of the dependent variable than the constant-only model. As seen in Table 6, right BA 32 was significant at $p < 0.01$, but had a standardized beta coefficient of -1.039. While standardized beta coefficients are assumed to be less than 1, there are instances where they can exceed 1, such as in the case where two or more predictors are highly correlated (Deegan, Jr., 1978). However, left BA9 has a standardized β of -0.163, and is significant at the $p < 0.01$ level. Thus, hypothesis 7a was supported. Tolerance values were also above 0.10 and VIF values below 10, indicating that multicollinearity may not have been a problem in this model.

Table 6. Regression Model for Dependent Variable of Trust (right BA47)

Independ-ent Variable	**Beta Coeffici-ent**	**Standardiz-ed Beta Coefficient**	**Significan-ce (t-value)**	**Signific-ance (p-value)**	**Toleran-ce**	**VIF**
Right BA 32	0.960	-1.039	-18.042	0.000***	0.174	5.76
Left BA 9	-0.153	-0.163	-2.822	0.005**	0.174	5.76

5.4.2. Regression Model for Personal Information Disclosure

The dependent variable, personal information disclosure was regressed against the independent variables, Right BA 32, Left BA 9, Right BA 47, Right BA 31, Right BA 13, Left BA 40, Left BA 37, and privacy concerns. The regression model had an R-square value of 0.483 (R^2 = 0.483), with an adjusted R-square value of 0.471. The R-square and adjusted R-square values indicated the variance predicted by the independent variables in the model was fair enough. Specifically, R-square values when predicting human behavior are not always extremely high. The adjusted R-square value for this regression model of 0.471 is close to the adjusted R-square value of Dimoka's (2010) regression model of 0.49. The regression model had an F-value of 40.05 ($p < 0.001$), indicating that the independent variables significantly predicted the dependent variables. Table 7 displays the regression coefficients of the independent variables on personal information disclosure.

Table 7. Regression Model for Dependent Variable of Personal Information Disclosure

Independent Variable	**Beta Coefficient**	**Standardized Beta Coefficient**	**Significance (t-value)**	**Significance (p-value)**	**Tolerance**	**VIF**
Right BA 32	-0.464	-0.228	-2.016	0.045*	0.074	13.5
Left BA 9	0.404	0.246	2.434	0.015*	0.147	6.79
Right BA 47	0.501	0.287	2.890	0.004**	0.153	6.55
Right BA 31	0.084	0.053	0.489	0.646	0.113	8.85
Right BA 13	-0.413	-0.253	-2.532	0.012*	0.151	6.61
Left BA 40	-0.169	-0.103	-1.120	0.227	0.209	4.78
Left BA 37	0.201	0.109	2.097	0.037*	0.561	1.78
Privacy Concerns	-0.830	-0.683	-17.104	0.000***	0.945	1.06

* $p \leq 0.05$, ** $p \leq 0.01$, *** $p \leq 0.001$

Apart from the right BA 31 and left BA 40, all Brodmann Areas were significantly related to personal information disclosure. As indicated in the results from experiment 1, privacy concerns are related to brain activity in both the right BA32 and left BA 9. Right BA 32 has a significant and negative relationship with personal information disclosure (standardized $\beta = -0.228$, $p < 0.05$), indicating that an increase in brain activity in the right BA 32 is related to a decrease in an individuals' decision to disclose his/her personal information. The results of BA 32, when regressed on personal information disclosure partially supports hypothesis 6b. However, left BA 9 has a positive relationship with personal information disclosure (standardized $\beta = 0.246$, $p < 0.05$), whereby an increase in an individual's decision to disclose personal information is related to an increase in brain activity in the left BA 9. Similarly, right BA 47, the associated neural correlate for trust, also has a significant and positive relationship with personal information disclosure (standardized $\beta = 0.287$, $p < 0.01$), supporting hypothesis 7b.

Right BA 31, one of the neural correlates for distrust, had a positive relationship with personal information disclosure; however, the relationship was not significant. The other neural correlate for distrust, the insula cortex, BA 13, had a negative relationship with personal information disclosure, with a standardized $\beta = -0.253$ ($p < 0.05$). Essentially, an increase in brain activity in BA 13 is related to a decrease in personal information disclosure. Hypothesis 8b is thus partially supported based on the result of BA 13 on personal information disclosure. Left BA 40 and 37 are associated with a high level of an individual's personal interest, and both had positive beta coefficients, indicating an increase in BA 40 or BA 37 would increase an individual's decision to disclose personal information. However, only BA 37 was significant, with a standardized $\beta = 0.109$. Hypothesis 9 was thus partially supported. Privacy concerns, were negatively and significantly related to personal information disclosure, with a standardized $\beta = -0.683$ ($p < 0.001$), indicating an increase in privacy concerns will cause a decrease in personal information disclosure, supporting hypothesis 11. Tolerance and VIF values were collected for each variable, whereby each variable, apart from BA 32 were above the 0.10 threshold for tolerance, and below the 10 threshold for VIF indicating multicollinearity may not be present.

Table 8 displays the interaction effects of independent variables on the dependent variable of personal information disclosure that were significant at $p \leq 0.05$. The results from Table 8 supports hypothesis 12b, in that interaction effects would occur. In total, there are twelve interaction effects, with beta coefficients used to explain how much change occurs in the dependent variable based due to interactions between the independent variables.

Table 8. Significant Interaction Effects

Interacting Variables	**Beta Coefficients**	**Significance (t-values)**	**Significance (p-values)**
BA9L:BA47R:BA13R	-5.49	-2.046	0.0432*
BA47R:BA31R:BA40L:Privacy Concern	-5.62	-2.07	0.0409*
BA32R:BA9L:BA37L:Privacy Concern	1.36	2.211	0.0292*
BA31R:BA13R:BA37L:Privacy Concern	1.64	2.102	0.038*
BA9L:BA47R:BA31R:BA13R:BA40L	-1.33	-2.044	0.0435*
BA32R:BA9L:BA47R:BA40L:BA37L	1.68	2.045	0.0434*
BA32R:BA9L:BA13R:BA40L:BA37L	-9.28	-2.241	0.0271*
BA32R:BA9L:BA31R:BA40L:Privacy Concern	-1.47	-2.139	0.0347*
BA47R:BA31R:BA13R:BA37L:Privacy Concern	-7.00	-2.118	0.0366*
BA32R:BA9L:BA31R:BA13R:BA40L:BA37L	-2.20	-2.153	0.0336*
BA9L:BA47R:BA31R:BA13R:BA40L:Privacy Concern	-2.20	-2.153	0.0336*
BA32R:BA9L:BA13R:BA40L:BA37L:Privacy Concern	-2.36	-1.992	0.049*

* $p \leq 0.05$, ** $p \leq 0.01$, *** $p \leq 0.001$

5.5. Experiment 3: 2x1 Factorial Experiment

The current source densities for the ROIs for uncertainty and personal interest were extracted using sLORETA for the 2x1 factorial experiment, where uncertainty had one level, and personal interest had two levels (high and low). The average (log) CSD per ROI were then placed in regression models against privacy concerns, and personal information disclosure. The regression model for privacy concerns had an R-square of 0.072 and an adjusted R-square of 0.024. These values were low in predicting the dependent variable of privacy concerns. However, the model had an insignificant F-value of 0.753 ($p = 0.562$). The relationship between uncertainty (right BA's 40 & 47) and privacy concerns was not significant, neither were the relationships between personal interest (left BA 40 and BA 37) and privacy concerns. Thus, hypothesis 10a was rejected.

For the regression model against personal information disclosure, an R-squared of 0.438 and an adjusted R-squared of 0.364 was achieved suggesting a fair degree of predicting the dependent variable (personal information disclosure). The model also had an F-value of 5.930 ($p < 0.001$). However, similar to the privacy concerns model, neither the brain areas associated with uncertainty (right BA 40 and right BA 47) nor those of personal interest (left BA 37 and 40) were significant. Hypothesis 10b was thus rejected. However, privacy concerns were significantly and negatively related to personal information disclosure (standardized $\beta = -0.618$, $p < 0.001$), supporting hypothesis 11, as in experiment 2. Additionally, there were no significant interaction effects between the neural correlates of uncertainty and personal interest on either privacy concerns or personal information disclosure. Table 9 summarizes the results for the privacy concerns regression model, while Table 10 summarizes the results for the personal information disclosure regression model.

Table 9. Experiment 3: Regression for Privacy Concerns

Variabl-es	Beta Coeffici-ent	Standardiz-ed Beta Coefficient	Significa-nce (t-values)	Significanc-e (p-values)	Toleran-ce	VIF
BA 40R	-0.150	-0.142	-0.382	0.705	0.171	5.84
BA 47R	0.149	0.121	0.397	0.693	0.257	3.89
BA 40L	1.680	1.379	1.547	0.130	0.030	33.3
BA 37L	-1.699	-1.351	-1.562	0.126	0.257	31.4

Table 10. Experiment 3: Regression for Personal Information Disclosure

Variabl-es	Beta Coeffici-ent	Standardiz-ed Beta Coefficient	Significan-ce (t-values)	Significan-ce (p-values)	Toleranc-e	VIF
BA 47R	0.411	0.229	0.952	0.347	0.256	3.91
BA 40R	0.274	0.179	1.608	0.547	0.171	5.86
BA 40L	-0.215	0.121	0.167	0.868	0.028	35.4
BA 37L	-0.119	-0.065	-0.092	0.927	0.030	33.4
Privacy Concerns	-0.901	-0.618	-4.853	0.000	0.928	1.08

5.6. Summary

Paired groups zero-means t-tests using SnPM were conducted for experiment 1 to identify the neural correlates of the mental processes of privacy risk, trust, distrust, uncertainty and personal interest. The results of experiment 1 revealed that risk perceptions are associated with brain activity in right BA 32 and left BA 9, while trust perceptions are associated with right BA 47. Distrust perceptions are associated with brain activity in the right BA's 31 and 13, while uncertainty and personal interest perceptions are associated with right BA's 40 and 47, and left BA's 40 and 37, respectively. Experiment 1 supported hypotheses 1c, 3b, 4a and 4b.

For experiment 2, the average log CSD of ROI for each brain area identified in experiment 1 for each subject of the sixteen conditions were plugged into a regression model with the dependent variable of privacy concerns. The results indicated the model was a bad fit, and the only neural correlate that predicted privacy concerns was BA 13. However, this result is opposite to what was predicted in hypothesis 8a. Hypothesis 7a was assessed by developing a regression model for the dependent variable of the neural correlate trust (left BA 47) against the independent variables of the neural correlates for risk (right BA 32 and left BA 9). Hypothesis 7a was partially supported. The results of the regression model when plotted against a dependent variable of personal information disclosure found right BA's 32, 47, and 13, and left BA's 9 and 37 predicted personal information disclosure, as well as privacy concerns. Hypotheses 6b, 8b, and 9 were partially supported, while hypotheses 7b and 11 were fully supported. Also, there was a total of twelve significant interactions between the independent variables on the dependent variable of personal information disclosure. Therefore, while hypothesis 12a was rejected, 12b was supported. For experiment 3, for both the regression models against privacy concerns and personal information disclosure, there were no significant main or interaction effects, thus hypothesis 10a and 10b were rejected.

Chapter 6

Discussion

6.1. Introduction

This chapter discusses the results of the study, the contributions, as well as limitations and future research. Section 6.2 discusses the findings with regards to literature, while section 6.3 discusses the contributions of the study. Section 6.4 discusses the managerial implications derived from the results of this study, while section 6.5 discusses limitations and section 6.6 suggests future studies. Section 6.7 then concludes the dissertation, with summary of the overall study.

6.2. Findings

This study investigated the privacy paradox to better understand individuals' decision to withhold or disclose their personal information. The privacy paradox is explained as the concerns individuals express over the privacy of their personal information, yet act contrarily by continually disclosing their personal information (Smith et al., 2011). Extant literature has found that while privacy concerns often have a significant and negative relationship to the use of various ICTs (Anderson & Agarwal, 2009; Awad & Krishnan, 2006; Dinev & Hart, 2006; Xu et al., 2010), numerous other factors such as trust, personality, and culture plays an important role in shaping individuals decisions to disclose or withhold their personal information (Bansal et al., 2010; Belanger et al., 2002; Dinev et al., 2006). However, many studies have often assumed that privacy-related decisions, and therefore, the privacy paradox, could be explained by investigating individuals' rational decision-making processes (Dinev et al., 2006; Malhotra et al., 2004; Norberg et al., 2007; Pavlou et al., 2007; Van Slyke et al., 2006). Yet, individual' decisions are not completely rational, nor are they fully aware of all the parameters to make a completely justifiable decision in the context of information privacy (Acquisti & Grossklags, 2005).

Individuals' privacy-related decisions may in fact be clouded by emotions, that may not be reflective of a true calculus based on rewards and losses. Studies done by Acquisti (2004); Anderson and Agarwal (2011); and Li et al. (2011) establishes that individuals' decisions are limited by their cognitive capabilities and can be often affected by emotions. Moreover, as all decisions are based on cognitive processing of the human brain, findings in the field of cognitive neuroscience reveals that many decision-making processes are distinct from one another, and may involve a heavy mixture of rationality and emotion (Dimoka et al., 2007; 2011). Thus, to better understand the privacy paradox, this study argued that privacy-related decisions are based on an individual's cognitive disposition, which includes both rationality and emotions.

This study used the extended privacy calculus model (Dinev & Hart, 2006) as the theoretical basis, and applied the findings of cognitive neuroscience to it, to address its limitations in assuming individuals are rational decision-makers. Three within-subjects experiments were conducted to test the hypotheses and research model developed to achieve the objective of this study. There was a total of twenty-two subjects that participated in the experiments, but each subject participated in all three experiments as if they were one experiment. Table 11 summarizes the hypotheses for experiment 1 that were rejected and supported for this study.

Table 11. Results of Hypotheses Testing for Experiment 1

Hypothesis		Support
1a	Privacy Risk is associated with brain activity in the nucleus accumbens	Not Supported
1b	Privacy Risk is associated with brain activity in the insula cortex	Not Supported
1c	Privacy risk is associated with brain activity in anterior cingulate cortex	Supported
2a	Trust is associated with brain activity in the caudate nucleus	Not Supported
2b	Trust is associated with brain activity in the putamen	Not Supported
3a	Distrust is associated with brain activity in the amygdala	Not Supported
3b	Distrust is associated with brain activity in the insula cortex	Supported
4a	Uncertainty is associated with brain activity in the orbitofrontal prefrontal cortex	Supported
4b	Uncertainty is associated with brain activity in the inferior parietal cortex	Supported
5a	Personal Interest is associated with high brain activity in the ventromedial prefrontal cortex, but low activity in the dorsolateral prefrontal cortex	Not Supported
5b	Personal Interest is associated with brain activity in the inferior parietal lobule	Supported

While several hypotheses were not supported in experiment 1, this was expected as many of these hypotheses were derived from fMRI and PET literature. EEG captures electric potentials in the human brain, while fMRI and PET measure blood oxygen level dependent (BOLD) signals in the brain. Furthermore, EEG provides greater temporal resolution at the cost of spatial resolution, and vice versa for fMRI and PET (Riedl et al., 2009). However, despite the lack of support for many of the hypotheses, findings for key brain areas involved in the mental processing of factors such as privacy risk, trust, distrust, uncertainty and personal interest were found. Privacy risk found brain activity in the right BA 32 (anterior cingulate cortex), as well as in the frontal lobe of left BA 9. Right BA 47, which constitutes a part of the orbitofrontal prefrontal cortex was involved in trust, while distrust included the right BA 31. Additionally, the neural correlates of personal interest were found to be left BA 40, the inferior parietal lobe, and left BA 37, the middle temporal gyrus in the temporal lobe. Figure 14 depicts the research model of neural correlates with the relationships that were supported (denoted with an *), while figure 15 depicts the research model with significant relationships (denoted by * for partial support and ** for full support) to personal information disclosure. The hypotheses for experiments 2 and 3 are summarized in Table 12, which are discussed in detail in the following subsections.

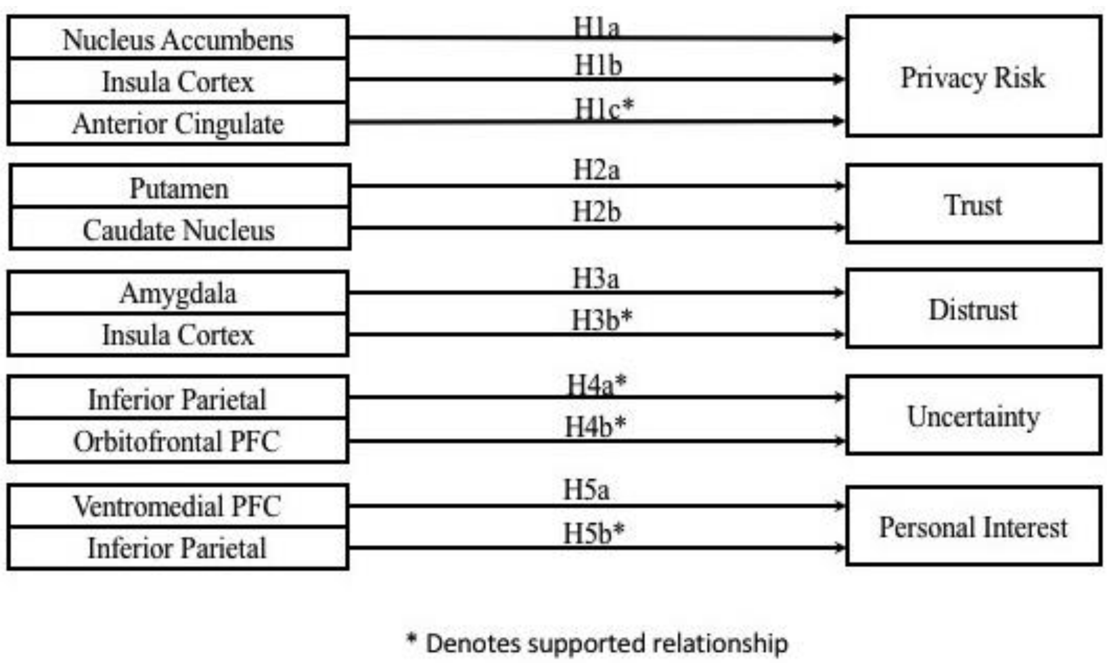


Figure 14. Research Model depicting Significant Neural Correlates of Mental Processes

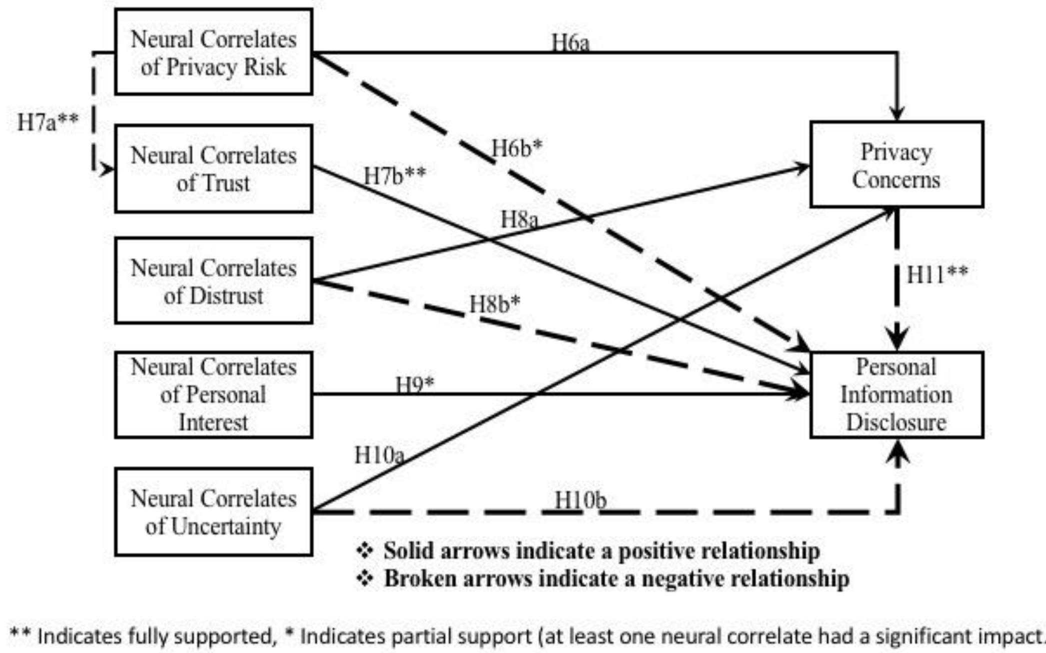


Figure 15. Research Model with Supported Hypotheses

Table 12. Results of Hypotheses Testing for Experiments 2 and 3

Hypotheses		Neural Correlates	Standardized β (p-value)	Support
6a	The neural correlates of privacy risk are positively related to privacy concerns	rBA32 lBA9	$0.317^{N.S.}$ $-0.055^{N.S.}$	Not Supported
6b	The neural correlates of privacy risk are negatively related to personal information disclosure	rBA32 lBA9	-0.228* 0.246*	Partially Supported
7a	The neural correlates of privacy risk are negatively related to the neural correlates of trust	rBA32 lBA9	-1.039*** -0.153**	Supported
7b	The neural correlates of trust are positively related to personal information disclosure	lBA47	0.287**	Supported
8a	The neural correlates of distrust are positively related to privacy concerns	rBA31 rBA13	$0.247^{N.S.}$ -0.294*	Not Supported
8b	The neural correlates of distrust are negatively related to personal information disclosure	rBA31 rBA13	$0.053^{N.S.}$ -0.253*	Partially Supported

9	The neural correlates of personal interest are positively related to personal information disclosure	lBA40 lBA37	-0.103$^{N.S.}$ 0.109*	Partially Supported
10a	The neural correlates of uncertainty are positively related to privacy concerns	rBA40 rBA47	-0.142$^{N.S.}$ 0.121$^{N.S.}$	Not Supported
10b	The neural correlates of uncertainty are negatively related to personal information disclosure	rBA40 rBA47	0.229$^{N.S.}$ 0.179$^{N.S.}$	Not Supported
11	Privacy concerns are negatively related to personal information disclosure	*N.A.*	-0.683***	Supported
12a	An interaction effect would exist between the independent variables and privacy concerns	*N.A.*		Not Supported
12b	An interaction effect would exist between the independent variables and personal information disclosure	*See Table 8 of Chapter 5*		Supported

N.S. Not Significant, * p ≤ 0.05, ** p ≤ 0.01, *** p ≤ 0.001, r Right, l Left

6.2.1. Privacy Risk

Privacy risk was found to be associated with the right BA 32 which is part of the anterior cingulate cortex. Similar results were found by Massar et al. (2012) when studying individuals with risk-taking and risk-aversive behavior. The anterior cingulate cortex is in the limbic lobe which controls emotions (Dimoka et al., 2007). Studies have found the anterior cingulate was involved in processing of emotions (Allman, Hakeem, Erwin, Nimchinsky, & Hof, 2001; Beuregard, Levesque, & Borgouin, 2001). While risk in the information privacy literature has often been treated as one-dimensional, it may be a multidimensional construct that assesses loss and considers the outcomes of avoiding a risk (Peter & Tarpey, 1975; Smith et al., 2011). Risk-avoidance behavior was reported to have been associated with brain activity in the nucleus accumbens, which is considered a reward center of the brain (Knuston et al., 2001; Matthews et al., 2004). Similarly, the anterior cingulate was reported to be active during assessments of rewards (Bush, Vogt, Holmes, Dale, Greve, Jenike, & Rosen, 2001).

The results of experiment 1 also found left BA 9 was activated during processing of privacy risk perceptions. BA 9 has been shown to be associated with both pleasant and unpleasant emotions (Lane, Reiman, Bradley, Lang, Ahem, Davidson, & Schwartz, 1997). The left BA 9 is considered a part of the dorsolateral prefrontal cortex, along with BA 46 (Pochon et al., 2001). The dorsolateral prefrontal cortex is considered one the most advanced areas of the human brain and is often involved in high cognitive functions (Dimoka et al., 2011). Furthermore, the cognitive neuroscience literature indicates that there seem to be some level of interaction between the right and left dorsolateral prefrontal cortices and the anterior cingulate, since they have been involved in attentional and executive tasks (Bench et al., 1993; Posner & Rothbart, 1998).

Essentially, privacy risk may be assumed to involve both the risk and reward centers of the brain, and may consist of a high degree of emotions. However, given that there is a great deal of interaction between emotional processing, and rationality (Phelps, 2006), it can also be assumed that there is some degree of rationality to processing of risk in the context of information privacy. As explained by Demos (2005), when an individual experiences a real or imagined threat, it is first recorded by the thalamus, which sends two signals, firstly to the limbic system, and secondly to the executive portions of the frontal lobe. The processing of a threat leads to neurochemical responses, which may be shut down by the executive centers of the brain if the threat is recognized as false. Essentially, privacy risk may be the similar whereby emotions are triggered to avert a risk, while the executive portions of the brain manages this emotion and responds accordingly. In such a case, individuals' actions could thus be classified as risk-aversive or risk-taking.

When both right BA 32 and left BA 9 were regressed against privacy concerns, neither brain areas were significant predictors. These findings contradict the findings of Dinev et al., (2004; 2006) and Van Slyke et al. (2006), which used self-reported findings. However, as the data collected were perceptions based on the processing of stimuli as opposed to the enduring beliefs of risk, it is not surprising to find the results are different. The results also suggest that privacy risk may be understudied in the information privacy field and may require further investigations with regards to privacy concerns. There were, however, significant relationships between the neural correlates of privacy risk and personal information disclosure. The anterior cingulate cortex (right BA 32) did predict a decrease in personal information disclosure, however, the left BA 9 predicted an increase in personal information disclosure. Furthermore, the results of left BA 9 are consistent with the association of left prefrontal cortex in dominating positive emotions (Hellige, 1993). Left BA 9 had a stronger effect that right BA 32 in personal information disclosure with a standardized β of 0.246 as opposed to -0.228. This does not necessarily mean the neural correlates of risk perceptions contradict each other when predicting personal information disclosure. Rather, privacy risk may involve both the processing of losses and rewards in each privacy-related situation, which may involve the risk-taking and risk-aversion behaviors of individuals.

When regressed against the neural correlate of trust (right BA 47), both neural correlates of risk were significant. An increase of neuronal activity in either the right BA 32 or left BA 9 led to a decrease in neuronal activity in the right BA 47, the neural correlate of trust. Furthermore, standardized beta coefficients of the right BA 32 had a stronger effect than left BA 9. Essentially, the inference could be made that increased brain activity in regions associated with privacy risk could lead to decreased activity in brain areas associated with trust.

6.2.2. Trust

Trust perceptions were associated with right BA 47, which constitutes a part of the orbitofrontal prefrontal cortex (Kringelbach, 2005). This is contrary to the results found by Dimoka (2010) who found that trusting situations led to a decrease in brain activity in the orbitofrontal prefrontal cortex. However, Rogers et al. (1999) found that the regions within the orbitofrontal prefrontal cortex (specifically, BA 47) may be involved in processing changes in reward-related information. It can be assumed, therefore, that deciding to withhold or disclose personal information, the neural correlate of trust, BA 47 is activated for estimating the likelihood of reaping rewards in privacy-related transactions.

The orbitofrontal prefrontal cortex is involved in several mental processes, such as emotional regulation, self-regulation and most cognitive processes (Cannon, 2012). BA 47 has been found to be associated with the assessment of rewards and higher emotional valence, along with other brain areas such as BA’s 24 (anterior cingulate) and the putamen (Hollander, Pallanti, Baldini, Sood, Baker, & Buchsbaum, 2005). When regressed against personal information disclosure, right BA 47 was significant, and the second highest effect among the other variables, with a standardized beta coefficient of

0.287. Essentially, these results indicated that an increase in the neural correlate of trust perceptions led to an increase in individuals' decision to disclose personal information.

6.2.3. Distrust

Distrust activated distinct areas of the brain as opposed to trust. Where trust activated right BA 47, distrust activated right BA 31, the posterior cingulate, and BA 13, the insula cortex. These results were aligned with the results of Dimoka (2010) in proving that trust and distrust did not lie along a single continuum. Furthermore, the activation of the insula cortex corroborates the findings of Dimoka (2010) that found distrust was correlated with brain activity in the amygdala and insula cortex. The insula cortex is more active in affective/emotional choices, as opposed to cognitive processes, and is often involved in strong negative emotional processing (Cannon, 2012; Dimoka, 2010; Sawamoto et al., 2000).

The right BA 13 was significant in predicting privacy concerns, however, the relationship indicated that an increase in right BA 13 led to a decrease in privacy concerns. These findings were contrary to the hypothesis, indicating more investigation is needed in better understanding privacy concerns. The right BA 13 did have a negative relationship with personal information disclosure, with a standardized beta coefficient of -0.253. When compared to the effect of the neural correlate of trust, right BA 13 had a weaker effect. This contradicts the findings of Dimoka (2010), who found distrust was more salient than trust in deciding price premiums. However, given that this study focused mainly on the disclosure of personal information, as opposed to money, it is possible that individuals' judgments are different. Specifically, the loss of money may trigger stronger negative emotions than the probable loss of privacy, similar to the findings of Hollander et al. (2005), where monetary value consisted of more brain activity in regions of high risk and high reward, as opposed to a computerized game point system.

Activation was found in the right BA 31, the posterior cingulate. The posterior cingulate cortex is involved in emotional processing, and as an evaluative region of the brain, that is involved in assessing environmental stimuli and memory functions (Vogt, Finch, & Olson, 1992). However, it is also involved in evaluative judgements, i.e. making an assessment to determine the quality of something (Zysset, Huber, Ferstl, & von Cramon, 2002). Yet, no significant relationships were established between right BA 31 and privacy concerns nor personal interest.

6.2.4 Uncertainty

The hypotheses were supported for assessing the neural correlates of uncertainty, which were found to be right BA 47 and right BA 40. As discussed above, the right BA 47 is a part of the orbitofrontal prefrontal cortex that is often involved in both the processing of emotions and cognitive tasks. While right BA 47 was found as a neural correlate for trust, a positive mental process, neuronal activity and mental processes contain a many-to-many relationship (Dimoka, 2012). Studies have shown that activity in the right prefrontal cortex are often involved in processing unpleasant emotions (Davidson, 2002; Davidson, Coe, Dolski, & Donzella, 1999). Moreover, the orbitofrontal cortex was found to be involved in many cognitive and emotional thought processes (Cannon, 2012). Brain activity was also found in the right BA 40 is a part of the inferior parietal lobule, which is involved in attentional tasks, as well as processing of cognition and emotion (Cannon, 2012; Krain et al., 2006) for uncertainty.

The neural correlates of uncertainty were found to be insignificant predictors of privacy concerns and personal information disclosure. These findings are contrary to that of Pavlou et al. (2007) that found perceived uncertainty negatively impacted intentions to disclose personal information, highlighting the differences in results that are captured by neuroimaging tools as opposed to self-reported data. Additionally, these findings reinforce the position that brain areas and mental processes contain a many-to-many relationship, whereby right BA 47 was found significant for trust conditions, but insignificant for uncertainty conditions. Moreover, there may be similarities, in particular, the orbitofrontal prefrontal cortex, between the brain areas shared for assessing both rewards and punishments (Kringelbach & Rolls, 2004).

6.2.4 Personal Interest

Brain activity in the left BA 40 was found to be associated with personal interest, providing support for hypothesis 5b. The results are similar to consumer behavior, where the right BA 40 was activity, and along with high activity in the ventromedial prefrontal cortex, and low activity in the dorsolateral prefrontal cortex, suggested impulsivity (Deppe et al., 2005). Left BA 37 was also found to be active for personal interest. BA 37 is associated with visual recognition (Tanaka, 1997), but is also classified as a part of the temporal lobes which are involved in social and emotional processes, decision-making and has connections with the orbitofrontal cortex and amygdala (Dupont, 2002). Additionally, Leube, Erb, Grodd, Bartels, & Kircher (2001) found BA 37 to play a key role in episodic memory. When testing for personal interest, instead of presenting the subjects with random items, product categories (for ecommerce) and e-service categories were displayed for subjects to choose from. Subjects were asked to choose which category best represented their personal interest, as well as keeping this category in mind for the subsequent experiments. The findings of left BA 37 and the manner in which the study tested for personal interest, suggests that there was some degree of memory involved in selecting a product category.

When regressed against privacy concerns, neither left BA's 37 nor 40 had significant relationships. Similarly, left BA 40 was not found to have a significant relationship with personal information disclosure. However, left BA 37 was found to have a significant relationship with personal information disclosure, whereby an increase in left BA 37 would predict an increase in personal information disclosure. It should be noted, however, that based on the standardized β of 0.109, personal interest had the smallest effect as compared to the other independent variables on personal information disclosure.

6.2.5. Privacy Concerns

Privacy concerns as a dependent variable had poor predictors which were insignificant, and bad model fit. The only significant variable to have a relationship with privacy concerns was right BA 13, and the relationship was contrary to the hypothesis. However, data collected for privacy concerns utilized a one-item survey question of self-reported data. Essentially, privacy concerns, like privacy risk, have been found to be more complex and multidimensional, whereby researchers have developed instruments to properly assess privacy concerns (Malhotra et al., 2004; Smith et al., 1999). As such, a more appropriate means of assessing privacy concerns may have presented more insightful findings. Moreover, neural correlates of privacy concerns were not assessed, which may have provided useful insights as to how the human brain processes information privacy.

When regressed against personal information disclosure, privacy concerns were statistically significant, and had the strongest effect when compared to all the other independent variables, with a standardized beta of -0.683. This relationship indicated that when privacy concerns increased by one unit, there would be a decrease of the dependent variable, personal information disclosure by a standard deviation of -0.683. This negative relationship is consistent with findings in the information privacy field, where privacy concerns negatively impact the use of ICTs that require individuals to disclose their personal information (Awad & Krishnan, 2006; Bansal et al., 2010; Dinev & Hart, 2006; Pavlou et al., 2007; Van Slyke et al., 2006).

6.2.6. Interaction Effects

While experiment 3 did not produce any significant interaction effects, nor did the regression model with the dependent variable of privacy concerns for experiment 2, there were in total, twelve significant interactions between the independent variables for the dependent variable of personal information disclosure (see Table 8 in Chapter 5). In total, only three out of twelve interactions that had a positive relationship with personal information disclosure, each of which had beta coefficients higher than 1, but less than 2. Alternatively, all the significant interactions with negative relationships had a beta coefficient of -1.33 as its lowest, but -9.28 as the highest, which was an interaction between the neural correlates of privacy risk, distrust (only BA 13) and personal interest.

In all interactions where the independent variables positively predicted personal information disclosure, brain activity in left BA 37 (a neural correlate of personal interest) was present. The neural correlate of trust (right BA 47) often had little effect in predicting personal information disclosure. Interactions where both neural correlates of distrust and trust were present predicted a reduction of personal information disclosure (i.e. negative beta coefficients). These findings were similar to Dimoka (2010), which found distrust was more salient than trust in predicting price premiums. Additionally, the high number of interactions of the independent variables and their predicted negative relationships and magnitude (i.e. beta coefficients) with personal information disclosure reinforces the weight negative outcomes have over positive ones, when individuals make decisions regarding rewards and losses (Kahneman & Tversky, 1979).

6.3. Contributions

There were four contributions from this study to information privacy research. Firstly, this study provides a better explanation to the privacy paradox in that individuals' privacy-related decisions are based on both rational and emotional mental processes, that intertwine with one another. The findings thus supports the research argument that individuals disclosed their personal information based on their cognitive disposition. Essentially, individuals' decision to withhold or disclose their personal information cannot be explained through rational behavior, nor solely through emotional impulses. Furthermore, this study addressed a gap in current privacy literature where the processing of external stimuli was measured as predictors of privacy-related decisions, as opposed to internally held beliefs. The neural correlates of mental processes that were posited to affect privacy-related situations were identified using a neurological tool, the electroencephalogram. The findings of this study identified the nature of the mental processes involved in privacy-related decision-making. This led to the second contribution, where the findings of cognitive neuroscience was applied to the extended privacy calculus model to address its limitation in assuming individuals are rational decision-makers. The third and fourth contributions are methodological contributions by using sLORETA technique to identify the neural correlates of mental processes posited to be involved in explaining the privacy paradox, and using SnPM for the analysis. These contributions are discussed in more detail next.

6.3.1. Research Contributions

The first research contribution of this study, whereby the findings of this study supported the research argument that individuals would disclose their personal information based on their cognitive disposition, which includes both rational and emotional mental processes. The brain areas identified as neural correlates to the factors such as privacy risk, trust, distrust, and personal interest are responsible for rational/executive functions, emotions, emotional regulation, and calculation of rewards. Thus, a better explanation of the privacy paradox is derived based on the results of the significant relationships of this study, between the neural correlates of mental processes, privacy concerns, and personal information disclosure. This indicates that individuals' privacy-related decisions are neither purely emotional nor rational, as there exists interconnectivity between these brain areas as suggested by Phelps (2006). Essentially, the privacy paradox cannot be explained solely through a logical cost-benefit analysis or by examining individuals' emotions only. Furthermore, the results of this study were based on studying real behavior influenced by the momentary perceptions formed in privacy-related situations as opposed to self-reported data on individuals' beliefs concerning information privacy and personal information disclosure.

The constructs of privacy risk, trust, privacy concerns and personal interest in the extended privacy calculus model were modeled as enduring (institutional) beliefs individuals have in the context of information privacy, which influences individuals' decisions to withhold or disclose their personal information. Yet, these constructs have been found to be correlated with neural activity in specific regions of the brain when individuals are processing stimuli, i.e. they are produced based on situations and are more a 'state-of-mind at a given time' as opposed to an enduring belief (Dimoka et al., 2007; 2011; Sur & Sinha, 2009). Additionally, studies have found that the activation of brain areas when individuals are in a specific situation influences behavioral outcomes (Dimoka, 2010; Vance et al., 2014). As Dimoka et al. (2011) indicated, the use of neuroscience can advance the IS field. One such opportunity ~~occurs~~ where antecedents of IS constructs could be used to predict certain behavior and challenge past IS assumptions. The findings of this study fulfill this opportunity highlighted by Dimoka et al., (2011) where specific neural correlates, that included emotional responses and rational processes, significantly influenced individuals to disclose or withhold their personal information.

The second contribution of this study resulted from applying the findings of cognitive neuroscience to the theoretically enhance the extended privacy calculus model developed by Dinev and Hart (2006). The extended privacy calculus model is limited in assuming individuals are rational decision-makers. The constructs established in the extended privacy calculus model were mapped to brain areas of neural activity using the findings of cognitive neuroscience literature, which identified these mental processes as distinct. This led to challenging traditional assumptions such as the relationship between trust and distrust as existing along opposite ends of the same continuum. Mental processes such as uncertainty and distrust were therefore added to the extended privacy calculus model to better explain the privacy paradox.

As indicated by the results of this study, privacy-related decisions are not purely rational, and involves several brain areas related to assessments of risks and rewards, emotions, emotional regulations, and high executive processing. While the neural correlates of uncertainty did not have any significant relationships with privacy concerns or personal information disclosure, there were significant relationships with the neural correlates of privacy risk, trust, distrust and personal interest to personal information disclosure. Essentially, this study establishes distrust as an integral factor in the extended privacy calculus model, and explaining the privacy paradox. This study also advances the IS field as IS constructs were mapped to specific brain areas, which would allow for better understanding the nature and dimensionality of these constructs as opposed to utilizing the metrics of self-reported data that would be inadequate in assessing and understanding these constructs in privacy-related decisions (Dimoka et al., 2011).

6.3.2. Methodological Contributions

The third contribution of this study was related to the research methodology, and contributed to both the information privacy field, as well as NeuroIS in general. This study used (standardized) low tomography brain electromagnetic tomography to identify the neural correlates of mental processes posited to be involved in explaining the privacy paradox. While the use of PET and fMRI are considered better approaches to identifying the location of neural activity for given tasks, sLORETA provides specific advantages such as the increased temporal resolution of neuronal activity at specific moments in time (Cannon, 2012). The ability of sLORETA to capture neural activity in milliseconds addresses a fundamental limitation of fMRI research, where there are high degrees of overlap in brain areas during cognitive, affective, memory and attentional tasks, which leads to difficulty in accurately interpreting fMRI results (Cabeza & Nyberg, 2000). While sLORETA may have low resolution, it is able to detect neuronal activity in voxels of $5mm^3$, and detect even deeper brain structures such as the anterior cingulate cortex (Pizzagalli, Oakes, & Davidson, 2003), and hippocampal regions.

While there is a growing body of literature in the neuroscience field that utilizes sLORETA techniques for analysis of localization of brain areas for specific tasks, at the time of writing this dissertation, the use of sLORETA seems very rare in IS, with the only other study found utilizing sLORETA was that of Kalgotra, Sharda, and Chakraborty (2014). A search for the keywords “privacy”, “NeuroIS”, “Information Systems”, “LORETA” (with variations of “sLORETA”, “standardized LORETA”, “exact LORETA”, and “eLORETA”) did not return any results on databases such as ProQuest, ABI/InFORMs, and Web of Science for sLORETA-based research in IS, much less information privacy. The only result obtained from searching these databases with regards to neuroIS and information privacy returned an editorial calling for the use of neuroscience techniques in information privacy to better understand privacy constructs (Belanger & Xu, 2015).

Essentially, this study contributed by answering such a call to use neuroscience techniques to better understand the privacy paradox, while also contributing to NeuroIS by using sLORETA, a technique for identifying brain areas with high temporal resolution. Other than the analysis of the localization for key brain areas, sLORETA provides additional advantages such as the ability to provide analysis of frequency domains involved in specific tasks, along with localization (i.e. origination) of these frequency domains (Cannon, 2012; Massar et al., 2012). Furthermore, functional connectivity analysis can be done using sLORETA (Cannon, 2012), to determine "the temporal dependency of neuronal activation patterns of anatomically separated brain regions" (Lang, Tome, Keck, Gorriz-Saez, & Puntonet, 2012, p. 1).

An additional advantage of using sLORETA for identification of key brain areas entails the use of an EEG over an fMRI or PET, which reduces the monetary costs of collecting data drastically. Traditional neuroimaging tools such as fMRI and PET are very costly, with scans per subject for one-hour costing around $360-$540 and $450-$900, respectively (Riedl et al., 2009). EEG devices, in comparison, are much cheaper than purchasing fMRI and PET machines, while using the equipment from third parties (i.e. research labs and hospitals) can be as cheap as $55 per subject per hour (Riedl et al., 2009). Furthermore, the proliferation of commercial EEG devices such as emotiv EPOC+ and OpenBCI R&D kit, are much cheaper than traditional EEG devices, providing researchers with more cost-effective devices. This becomes an advantage for research, particularly in neuroIS and information privacy, since fMRI and PET studies have smaller sample sizes which can hinder the generalizability of findings (Dimoka, 2012). Yet, the use of EEG devices could provide more forms of analysis (i.e. frequency analysis, event-related potential component analysis), with localization determined through techniques such as sLORETA, with larger sample sizes. Additionally, the design of experiments becomes more flexible, whereby instead of constraining experiments to within-subjects designs to increase power while limiting sample sizes (Dimoka, 2012), a number of designs such as between-subjects and mixed designs (i.e. both a between and within-subjects design) can be used.

Finally, the forth contribution of this study was the use of SnPM for determining statistically significant brain areas involved in the mental processing of privacy-related decisions. Research in NeuroIS is limited, with a number of researchers appealing to the use of cognitive neuroscience to better understand information privacy (Dimoka et al., 2007; 2011; Riedl et al., 2009). Statistical Parametric Mapping (SPM) using general linear models is an often used approach of analysis for functional neuroimaging data, even in the fields of neuroscience and neuropsychology (Dimoka, 2012; Nichols & Holmes, 2001). In NeuroIS fMRI research, Dimoka (2010) used SPM to test for significant brain areas associated with trust and distrust. However, Nichols and Holmes (2001) explained that SnPM can surpass SPM for analyses of brain data with low degrees of freedom. Additionally, Pascual-Marqui et al. (2002) argued that SnPM was a powerful technique to accurately test the significance of brain areas produced from sLORETA, where parametric tests would be inadequate. Essentially, SnPM not only accurately analyzes data from sLORETA, but could also be used in the analysis of neuroimaging tools such as PET, fMRI, and single-photon emission computerized tomography (SPECT).

6.4. Managerial Implications

Several practices are suggested for both organizations and society. An organization's survivability and growth depends greatly on insights and predictions they gain from data mining techniques. This data allows for them to understand patterns and trends of their current clients as well as potential clients. However, acting opportunistically and selling data to third-parties or misrepresenting their practices of handling data could lead to a negative perception of the organization by society, such as in the case of ChoicePoint (Culnan & Williams, 2009). This can then lead to distrustful perceptions of an organization by society. As was evident in the case of ChoicePoint, this distrust of an organization could lead to major financial losses and loss of clientele. Organizations should therefore handle the personal information they collect from individuals with a high degree of ethical values (Culnan & Williams, 2009).

As can be seen from the findings, perceptions of trust and personal interest may consist of some degree of emotion targeting reward centers in the human brain, yet negative perceptions have more weight than positive ones. Thus organizations should reduce negative outcomes of privacy, in that the personal information they have collected and the data mining done to gain insights into client behavior should be handled carefully enough that negative reviews of an organization could easily be refuted (Mohammed & Tejay, 2015). Additionally, by acting in a manner that suggests an organization's ethical disposition as morally altruistic, with high concern and practices reflecting a "proactive privacy" attitude could lead to increased trust between clients and organizations. Organizations could achieve this by creating and often reviewing comprehensive privacy policies, developing a culture of privacy within an organization, designing informative and easy to read privacy statements, and helping individuals that were affected by privacy breaches overcome the negative outcomes (Culnan & Williams, 2009; Mohammed & Tejay, 2015). Organizations should also invest in messages, slogans, and cues that highlights the importance of clients' information privacy. As can be seen in cognitive neuroscience literature, as well as the findings in this study, specific stimuli trigger the neural activity associated with tasks. Essentially, creating positive messages to promote trusting perceptions and developing an environment of trust should impact individuals' privacy-related decisions and challenge minor negative privacy-related outcomes.

For individuals, privacy-related decisions have been found to include both a degree of emotions and rationality, with antecedents activating brain areas related to rewards, as well as negative emotions. This generally means that individuals' privacy-related decisions may not always reflect the best of judgements (Acquisti & Grossklags, 2005), and may also lead to taking risks in return for small rewards. Additionally, individuals may forego any rewards associated with specific ICTs due to fear of negative outcomes, which was found to have stronger weight in privacy-related decisions. To counteract many of these drawbacks, stronger regulations should be developed which balances the need for organizations and government to collect and analyze large sets of individuals' personal information, while limiting the probability of harm caused to individuals due to privacy and security incidents.

As ICTs are fast becoming a utility in everyday life (Buyya et al., 2008), maximizing the opportunities of ICTs should not be hindered by the risks in society. Privacy advocates could use the findings of this study pertaining to how individuals make privacy-related decisions, to form better campaigns to promote the development of fair privacy practices through campaigns by both governments and organizations. Furthermore, privacy advocates, as well as firms that specialize in information privacy and security could develop awareness programs centered around the perceptions found to influence privacy-related decisions in this study. These awareness programs could be used to aid individuals to make better privacy-related judgements, and promote the use of privacy enhancing technologies, such as Tor.

6.5. Limitations

There were a few limitations within this study. Firstly, privacy-related mental processes, such as privacy risk and privacy concerns have been discussed as multidimensional factors, with empirical evidence indicating privacy concerns are better modeled as second-order factor rather than a first-order factor (Smith et al., 2011; Stewart & Segars, 2002). In this study, neural correlates for privacy risk were assessed as if it were a completely negative factor, yet the findings indicated that while one of the neural correlates were negatively related to personal information disclosure (i.e. right BA 32), the other neural correlate (left BA 9) positively influenced individuals to disclose their personal information. These findings of privacy risk implied that privacy risk cannot be looked at as one single factor, with a single relationship to personal information disclosure, but may in fact pertain to the contradictory risk-behaviors of individuals who are considered either risk-taking or risk-aversive.

With regards to the findings of privacy concerns, none of the hypotheses posited to predict it were significant, which suggested that complex modeling of privacy concerns may be necessary to truly understand the nature of this construct. Additionally, privacy concerns may be correlated with specific brain areas by itself, and the self-reported metric used to determine a relationship within this study, was inadequate. However, privacy concerns did have the most significant effect on personal information disclosure, as well as the highest magnitude as compared to the other independent variables. This suggests the need for further investigation of mental processes such as privacy risk and privacy concerns.

Another limitation of this study was in the choice of the EEG device used to capture brain activity. The emotiv EPOC+ provided a cheaper solution as opposed to clinical EEGs, or functional neuroimaging tools such as fMRI and PET, but consisted of only fourteen electrodes. While sLORETA was chosen as the method to analyze the EEG data to derive the neural correlates of mental processes, some of the spatial resolution was sacrificed due to the limited number of electrodes. However, studies have shown that sLORETA can produce accurate results with a small number of electrodes (Cannon, 2012). While sLORETA can detect activity in deep brain regions such as the anterior cingulate (Pizzagalli et al., 2003), and other parts of the limbic lobe, such as the hippocampul gyrus, certain brain areas, such as the amygdala are more difficult to detect. In cases where such regions are of interest, high spatial resolution scans from fMRI and PET are recommended. However, both fMRI and PET contain poor temporal resolution, whereby brain areas activated for a given task become difficult to interpret due to the length of time passed since the stimulus was produced and the neural activity occurred (Cabeza & Nyberg, 2000). The results produced by sLORETA are in the millisecond range, where approximately every 7.8125 milliseconds, brain areas associated with specific tasks are captured for an EEG device with a 128Hz sampling rate. These sLORETA images can then be tested using SnPM for identifying statistically significant brain areas activated in the processing of certain stimuli.

It can be seen in the results that the statistics for assessing multicollinearity, the tolerance values were low, and the VIF values were high. However, despite this, all values for tolerance were above the minimum threshold, while VIF values were below the maximum threshold, except for right BA 32, in the regression model against personal information disclosure. This indicated that multicollinearity may not have been an issue in the study. However, even in the case of BA 32, multicollinearity does not invalidate the results of a regression model (O'Brien, 2007). Additionally, there is a high degree of connectivity in the brain, whereby, even if there were high correlations between the brain areas associated with mental processes, the functional connectivity of these areas alone cannot be decided simply through traditional multicollinearity tests, but may require connectivity analysis to better determine the degree of separation between the brain areas and their relationships. However, this was not an objective of this study.

Finally, this study did not account for differences in neural activity between right and left-handed individuals. Dimoka (2012) suggested limiting subjects to right-handed individuals when conducting fMRI experiments used for analyzing the neural correlates of mental processes. Gut et al. (2007) found that dominance of the right hand was controlled by the left hemisphere, while the non-dominant hand was controlled by both hemispheres of the brain. While investigations behind hand dominance and specific brain areas associated with perceptions of reward and losses are unclear, research does suggest that processing of motivation takes place in the hemisphere of dominance, i.e. right handed individuals had more activity in the left hemisphere and vice versa (Brookshire & Casasanto, 2012).

6.6. Future Research

There are a few studies that can be developed based on the findings and limitations of this study. Firstly, this study could be re-examined utilizing neuroimaging tools with higher spatial resolution, such as fMRI and PET. As research has found the mental correlates identified in this study to be correlated with some deeper brain structures such as the putamen and caudate nucleus for trust, amygdala for distrust, and nucleus accumbens for risk (Dimoka, 2010; Matthews et al., 2004), neuroimaging tools with higher spatial resolution may detect certain brain areas that were not detected in this study. Secondly, connectivity analysis, used for understanding the functional interconnectivity of neurons in specific brain areas could be used to better understand how the brain areas in this study are related to one another. This may in turn lead to inferences of the causal relationship between brain areas associated with privacy-related decisions, which is identified as one of the opportunities to advance the IS field by using the tools, techniques and theories from cognitive neuroscience (Dimoka et al., 2011).

Finally, a study on the differences on gender in privacy-related decision-making should be done. In this study, gender differences were not accounted for, however, studies in functional neuroanatomy suggest there are differences between brain activity in men and women. Dimoka (2010) found women had stronger neural activity in the emotional areas of the brain than men in trusting and distrusting situations. Essentially, the corpus callosum (connection between the right and left hemispheres) is thicker in women than in men, whereby women have about thirty percent more connectivity between the right and left hemispheres in the brain, and use both hemispheres for emotional processing, while for men, there are more activity in the right hemisphere for processing emotions (Pease & Pease, 2000).

6.7. Conclusions

As individuals are becoming more aware of the breaches information privacy, they have expressed a degree of privacy concerns, to which researchers have found were inhibitors to the use of ICTs (Li et al., 2011; Madden et al., 2007; Smith et al., 2011). Yet, despite expressing concerns over the privacy of their personal information, individuals continue to disclose their personal information; a behavior which is referred to as the privacy paradox. Researchers have often investigated the privacy paradox with regards to different ICTs, and found certain institutional beliefs, such as risk and trust were antecedents to explaining privacy-related decisions (Dinev & Hart, 2006; Pavlou et al., 2007; Van Slyke et al., 2005). However, a common assumption in information privacy research is that individuals are rational decision-makers. Acquisti and Grossklags (2005) argued that individuals are not able to make fully rational decisions, and their privacy-related decisions may be hindered by cognitive biases and limited cognition. Furthermore, a gap exists in the literature exists in observing how individuals’ perceptions are formed and relate to one another when they are in a situation requiring them to disclose their personal information. Specifically, the perceptions based on the cognitive processing of external stimuli, to which studies in neuroscience have indicated influence decision-making (Dimoka et al., 2007; 2011). Thus, the objective of this study investigated the privacy paradox to better understand why individuals disclose or withhold their personal information. The study argued that individuals disclose their personal information based on their cognitive disposition, which includes rationality and emotions.

The findings of cognitive neuroscience were applied to the extended privacy calculus model developed by Dinev and Hart (2006), addressing the limitation that individuals were rational in their privacy-related decisions. Three within-subjects experiments were carried out to test the research model and hypotheses. A total of twenty-two subjects participated in all three experiments as if it was one, while a pilot study was conducted using five participants. The first experiment assessed the neural correlates of mental processes involved in privacy-related decisions, while the second and third experiments were conducted to determine the effect of these neural correlates on privacy concerns and personal information disclosure. Experiment 2 was a 2x2x2x2 factorial experiment with high and low levels of personal interest, privacy risk, trust and distrust, leading to sixteen conditions in total, while experiment 3 was a 2x1 factorial experiment, with two conditions of a high and low level of personal interest and one high level of uncertainty. The results indicated that brain areas associated with emotional and rational functions, as well as emotional regulation, and risk and reward centers were involved in privacy-related decision-making.

The study contributed to the information privacy field by supporting the argument that individuals disclose their personal information based on their cognitive disposition. This challenges the past assumption of the privacy calculus in explaining the privacy paradox, and finding the nature and effect of neural correlates associated with mental processes that predict personal information disclosure. This lead to contributing theoretically to the information privacy field by applying the findings of cognitive neuroscience to the extended privacy calculus model, accounting for both rationality and emotions, while including distinct factors such as distrust and uncertainty. The study also contributed using sLORETA to identify the neural correlates associated with mental processes in privacy-related situations. Finally, using SnPM provides an alternate method of analysis with comparable results to parametric tests, especially in specific circumstances, such as in experiments with low degrees of freedom (Nichols & Holmes, 2001), which is a methodological contribution to information privacy research, and more broadly to the IS field.

Appendix A

IRB Approval Letter

MEMORANDUM

To: Zareef A Mohammed, MSc. Information Systems
College of Engineering and Computing

From: Matthew Seamon, JD, PharmD
IRB Chair, Institutional Review Board

Date: September 18, 2016

Re: 2016-393-The role of cognitive disposition in re-examining the privacy paradox: A
neuroscience study.

I have reviewed the revisions to the above-referenced research protocol by an expedited procedure. On behalf of the Institutional Review Board of Nova Southeastern University, *The role of cognitive disposition in re-examining the privacy paradox: A neuroscience study.* is approved in keeping with expedited review category # Expedited Category 4. Your study is approved on September 13, 2016 and is approved until September 12, 2017. You are required to submit for continuing review one month prior to September 12, 2017. As principal investigator, you must adhere to the following requirements:

1) CONSENT: You must use the stamped (dated consent forms) attached when consenting subjects. The consent forms must indicate the approval and its date. The forms must be administered in such a manner that they are clearly understood by the subjects. The subjects must be given a copy of the signed consent document, and a copy must be placed with the subjects' confidential chart/file.

2) ADVERSE EVENTS/UNANTICIPATED PROBLEMS: The principal investigator is required to notify the IRB chair of any adverse reactions that may develop as a result of this study. Approval may be withdrawn if the problem is serious.

3) AMENDMENTS: Any changes in the study (e.g., procedures,

consent forms, investigators, etc.) must be approved by the IRB prior to implementation.

4) CONTINUING REVIEWS: A continuing review (progress report) must be submitted by the continuing review date noted above. Please see the IRB web site for continuing review information.

5) FINAL REPORT: You are required to notify the IRB Office within 30 days of the conclusion of the research that the study has ended via the IRB Closing Report form.

The NSU IRB is in compliance with the requirements for the protection of human subjects prescribed in Part 46 of Title 45 of the Code of Federal Regulations (45 CFR 46) revised June 18, 1991.

Cc: Gurvirender P Tejay, Ph.D.
Ling Wang, Ph.D.

Institutional Review Board
3301 College Avenue Ft. Lauderdale, Florida 33314-7796
Phone: (954) 262-5369 Fax: (954) 262-3977 Email: irb@nova.edu Web Site: www.nova.edu/irb

Appendix B

Experimental Conditions

Experiment 1

Survey Questions per Condition

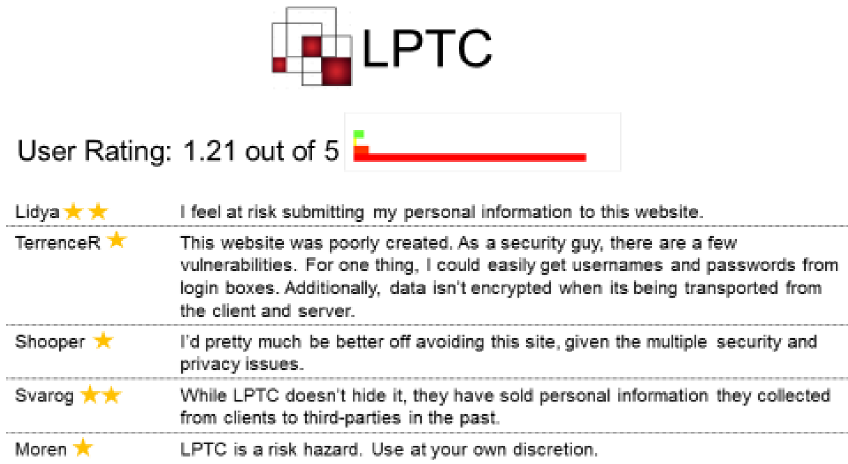
The following survey questions were asked after each subject read the review profiles:

Please rate on a scale of 1-7 the following items.
1 – Strongly Disagree; 2 – Disagree; 3 – Slightly Disagree; 4 – Neither Agree nor Disagree; 5 – Slightly Agree; 6 – Agree; 7 – Strongly Agree

1. Do you believe it is a risk to disclose personal information to LPTC?[1]
2. How likely are you to trust RTaP?[2]
3. Do you believe DisCV may not be completely honest?[3]
4. Are you uncertain about disclosing your personal information to IntraCOM?[4]
5. Are you personally interested in the product or service category you chose?[5]
6. How concerned are you about the privacy of your personal information when attempting to obtain a product or service online from this website?
7. How likely are you to disclose your personal information to obtain the product or service of your choice online from this website?

[1] For condition 1 only.
[2] For condition 2 only.
[3] For condition 3 only.
[4] For condition 4 only.
[5] For condition 5 only.

Condition 1 – Privacy Risk



Condition 2 – Trust

Condition 3 – Distrust

DisCV

User Rating: 1.21 out of 5

Djikstra ★	Collects a lot of personal information, and uses supercookies.
MiriamW ★★	I don't trust DisCV.
Mr.Smith ★	I feel as if I'm being lied too. DisCV doesn't have a bad reputation, per say, but their privacy practices are not adequate to warrant escape from a bad rep.
Quen ★★	There is a privacy policy, but it doesn't inspire confidence.
Dengeki-kun ★	I worked for DisCV, and left for a job at google about a year ago. At the time I was prohibited from saying anything, and I wouldn't risk even disclosing secrets on anonymous sites, just in case. DisCV is dishonest about how they use personally identifiable information. Now that I am free from their grip, I feel it is my ethical duty to advise others to avoid this website.

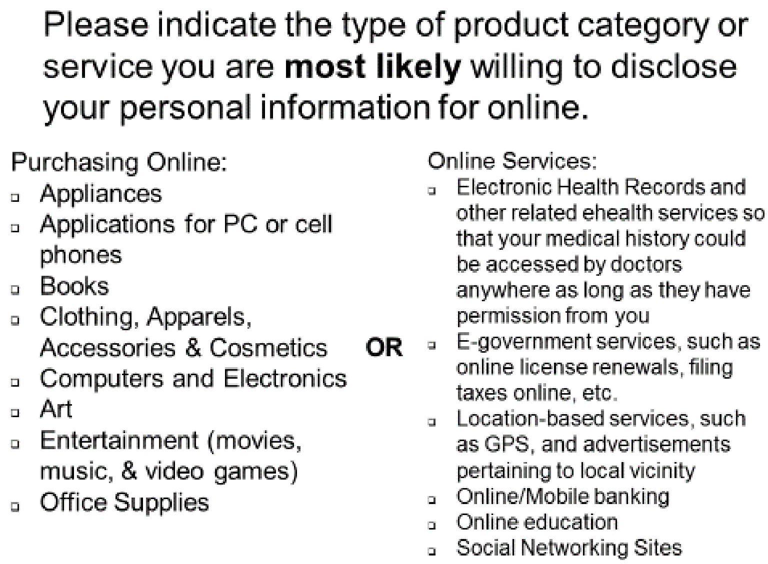
Condition 4 – Uncertainty

IntraCOM

User Rating: 2.66 out of 5

Reagan ★★★	I actually came here to see if anyone knows anything about this site. There is a privacy policy, but it doesn't really say anything….one line per section, no privacy seals, yet IntraCOM has been around for a while. Are they safe?
VaFieal ★★★	I was actually wondering the same as @Lacy. I mean, even there aren't even reviews for this site. Can someone please tell me if its safe to use IntraCOM?
ShinaYato ★★★	This site is very ambiguous. Not only does it have no appeal, no one seems to know much about the site to begin with.

Condition 5 – Personal Interest


Please indicate the type of product category or service you are **most likely** willing to disclose your personal information for online.

Purchasing Online:
- Appliances
- Applications for PC or cell phones
- Books
- Clothing, Apparels, Accessories & Cosmetics
- Computers and Electronics
- Art
- Entertainment (movies, music, & video games)
- Office Supplies

OR

Online Services:
- Electronic Health Records and other related ehealth services so that your medical history could be accessed by doctors anywhere as long as they have permission from you
- E-government services, such as online license renewals, filing taxes online, etc.
- Location-based services, such as GPS, and advertisements pertaining to local vicinity
- Online/Mobile banking
- Online education
- Social Networking Sites

Experiment 2

Survey Questions per Condition

The following survey questions were asked in each condition

Please rate on a scale of 1-7 the following items.
1 – Strongly Disagree; 2 – Disagree; 3 – Slightly Disagree; 4 – Neither Agree nor Disagree; 5 – Slightly Agree; 6 – Agree; 7 – Strongly Agree

1. Are you personally interested in the product or service category you chose?
2. Do you believe it is a risk to disclose personal information to (_____)[6]?
3. How likely are you to trust (_____)?
4. Do you believe (_____) may not be completely honest?
5. Are you concerned about the privacy of your personal information if you were to obtain a product or service online from (_____)?
6. How likely are you to disclose your personal information to obtain the product or service of your choice online from (_____)?

---

[6] The name of the simulated website/organization was placed in (_____), for each condition. For instance, condition 1 of experiment 2 was a review profile for “C-Sect”, thus in each question C-Sect for that condition was placed in place of the parenthesis.

Condition 1

C-Sect

User Rating: 2.98 out of 5

Erica ★★★★★	Extremely reliable and easy. I felt safe using this website.
Odym_Ares ★	This website is ridiculous, they're affiliated with a bunch of different companies that keep sending me advertisements in my email? I mean, why would they even give out my personal information?
~Siv:3 ★★	I've never heard of these guys before. Is it okay to use this website?
Nashi ★★★★★	Great and easy tool to get things done quickly.
KimReese ★	I don't trust this, I prefer to do things face to face.
MikeXD ★★★★	Works great. Easy to use, safe and secure.
tHat_IT_guy ★	I tried contacting them to opt-out, but couldn't. They have everything on me, this is scary.
WinDEX ★★★	I've seen good and bad reviews. Personally, never had a problem, but I am a bit skeptical.

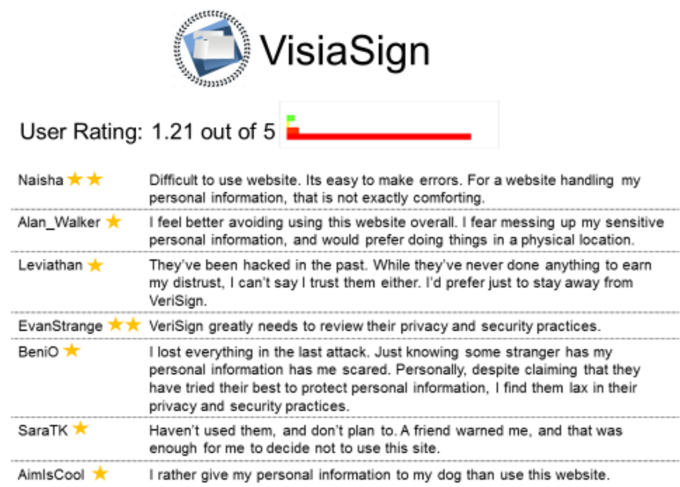
Condition 2

EsoCorp

User Rating: 1.18 out of 5

Illium ★	I do not feel safe using this website. They ask for too much info.
Rose ★	Recently saw an article online about how these website sells collected personal information.
FeVerNT ★★	What exactly are they using all the personal information they have collected about me? It's not as if half of these things relate to what I came here for.
Hack_theRipper ★	Tried deleting my account (unsubscribing). Was unsuccessful. Tried calling for support. No response.
WhiteOak ★	The quicker I can get out of here, the better. Too much information about me is collected.
Marcus ★★	After at least a month of trying, I finally got rid of my account. Still doesn't mean they don't have my personal information. They probably still do, which is a bit worrisome. Never again in here.
Nakajima ★	Like others have been saying.....bad website, bad support, too much info collected.

Condition 3



VisiaSign

User Rating: 1.21 out of 5

Naisha ★★	Difficult to use website. Its easy to make errors. For a website handling my personal information, that is not exactly comforting.
Alan_Walker ★	I feel better avoiding using this website overall. I fear messing up my sensitive personal information, and would prefer doing things in a physical location.
Leviathan ★	They've been hacked in the past. While they've never done anything to earn my distrust, I can't say I trust them either. I'd prefer just to stay away from VeriSign.
EvanStrange ★★	VeriSign greatly needs to review their privacy and security practices.
BeniO ★	I lost everything in the last attack. Just knowing some stranger has my personal information has me scared. Personally, despite claiming that they have tried their best to protect personal information, I find them lax in their privacy and security practices.
SaraTK ★	Haven't used them, and don't plan to. A friend warned me, and that was enough for me to decide not to use this site.
AimIsCool ★	I rather give my personal information to my dog than use this website.

Condition 4

HCCC

User Rating: 3 out of 5

Micheal ★★★	Can't really say anything good or bad about the site. No problems thus far.
Burns2o4 ★★★	At least they have a privacy policy. I'm very picky about these things, though it's not very well constructed.
Shivinan ★★★	I'll use this site…..but very carefully.
Lycus ★★★	There doesn't seem to be much issues with HCCC in terms of privacy or security, but they don't fill me with any confidence either.
WinterIsComing ★★	It's always better to do things face to face in my opinion. Though, I am willing to test out HCCC.
Hashirama ★★★	The main things I look out for when deciding to use the Internet and disclose my personal information are the privacy policies, and past incidents. HCCC has neither had any major privacy or security issues, but at the same time, it doesn't look like they are very proactive about privacy and security.
MitoX--X ★★★	I'm willing to disclose my personal info to HCCC, but I'll be careful.

Condition 5

Mass Relay Networks

User Rating: 1.42 out of 5

ElizaMasters ★	There privacy policy and privacy practices don't match. They claim to notify us about how our personal information is being used, yet they sell it to third-parties.
KenShindoi ★	Don't trust this site. They lie about how they handle personal information.
Ermac ★	There is relative assurance in knowing the third-parties Mass Relay Networks sell our personal information to are safe and secure, it is infuriating that they will even sell our personal information to begin with. Who knows when they might sell it to the wrong person.
KCWhitehall ★	I read a case study on their data mining of collected personal information. It was actually really dishonest and disgusting how much information they analyze about us. I don't recommend this to anyone.
FemiNash ★★	Trust is an important feature for me when I have to get into business and/or disclose my personal information to anyone. I have no trust in Mass Relay Networks.
LizCorvak ★★	Lots of bad rumors about how personal information is handled, as well as unfavorable reviews. At first I thought people were just complaining unnecessarily. Turns out they were right. Do not trust Mass Relay Networks.

Condition 6

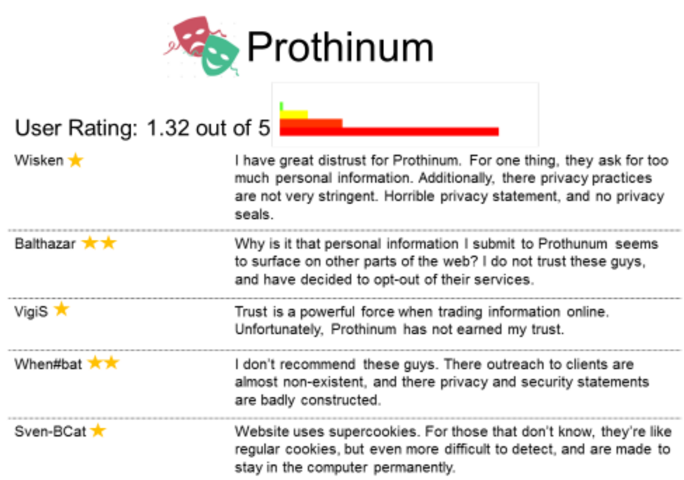
Yreden

User Rating: 2.96 out of 5

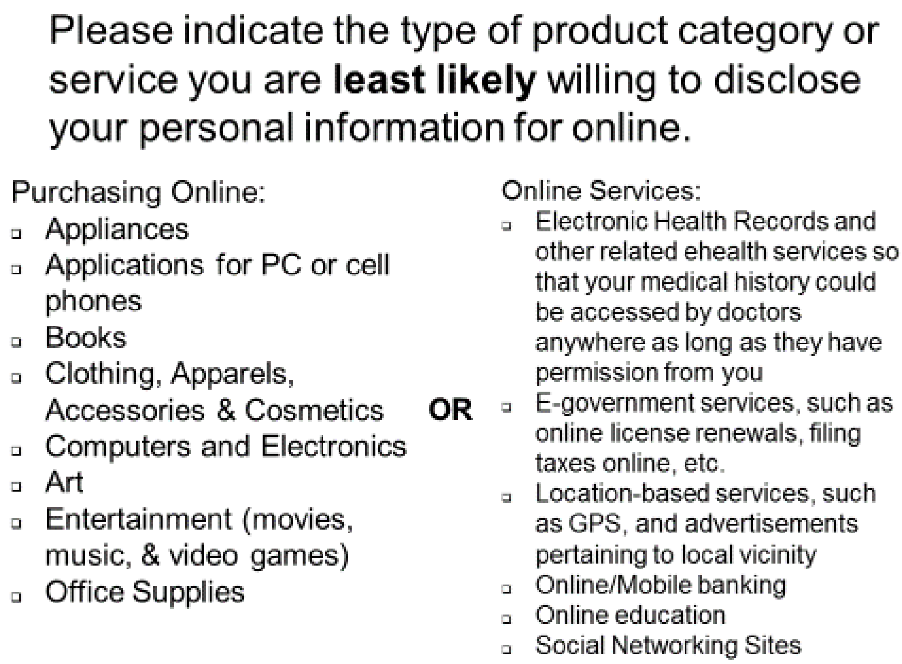
Elliot_S ★★★★	My experience with Yreden has been good thus far, but they aren't very forthcoming about their privacy practices. Their privacy policy is ambiguous.
RyderMC ★★★★★	Good service thus far, though they do gather a lot of personal information.
Hikkokimura ★★★	Why do they gather so much personal information? I mean, what's it being used for anyways? But, oh well, service with Yreden has been great so far, so I guess they are doing something right.
VincentBA ★★★★★	I recommend Yreden to everyone. Though I wish I knew why they gather soo much personal information.
Feroslo ★★★	While I rather do things with an actual person rather than through a virtual world, I'm not opposed to using Yreden.
lakeisgreener ★★★	Speaking professionally, Yreden takes information security seriously, and has never sold out their clients' personal information. But their privacy statements are really lacking in transparency, they don't use privacy seals, and they don't even try to connect with clients to assure them the plethora of personal information they have collected is actually safe and private.

Condition 7

Condition 8



The following screen appeared to change the level of Personal Interest to Low:



The same review profiles from conditions 1 to 8 in experiment 2 were repeated, under this condition of "Low Personal Interest", completing conditions 9 to 16.

Experiment 3

Survey Questions per Condition

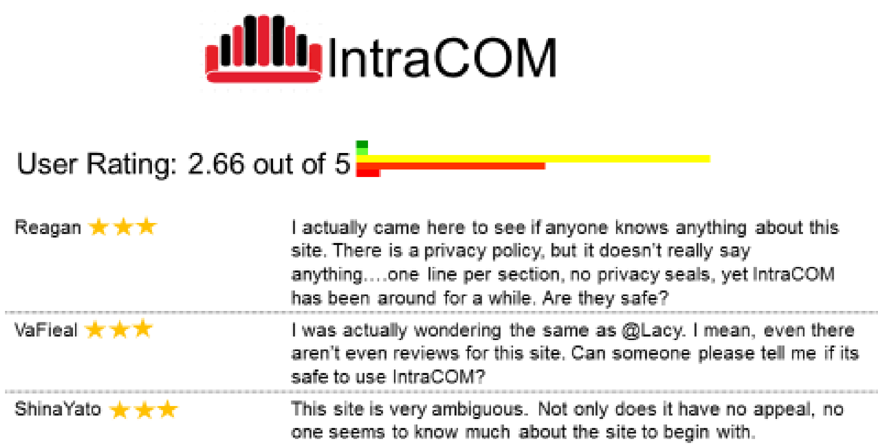
The following survey questions were asked in each condition

Please rate on a scale of 1-7 the following items.
1 – Strongly Disagree; 2 – Disagree; 3 – Slightly Disagree; 4 – Neither Agree nor Disagree; 5 – Slightly Agree; 6 – Agree; 7 – Strongly Agree

1. Are you personally interested in the product or service category you chose?
2. Are you concerned about disclosing your personal information to IntraCOM?
3. Are you concerned about the privacy of your personal information if you were to obtain a product or service online from (_____)?
4. How likely are you to disclose your personal information to obtain the product or service of your choice online from (_____)?

Condition 1 of experiment 3 followed on from the choice made in condition 5 of experiment 1, while condition 2 of experiment 3 followed on from the choice made in experiment 2 concerned with low personal interest.

Conditions 1 and 2



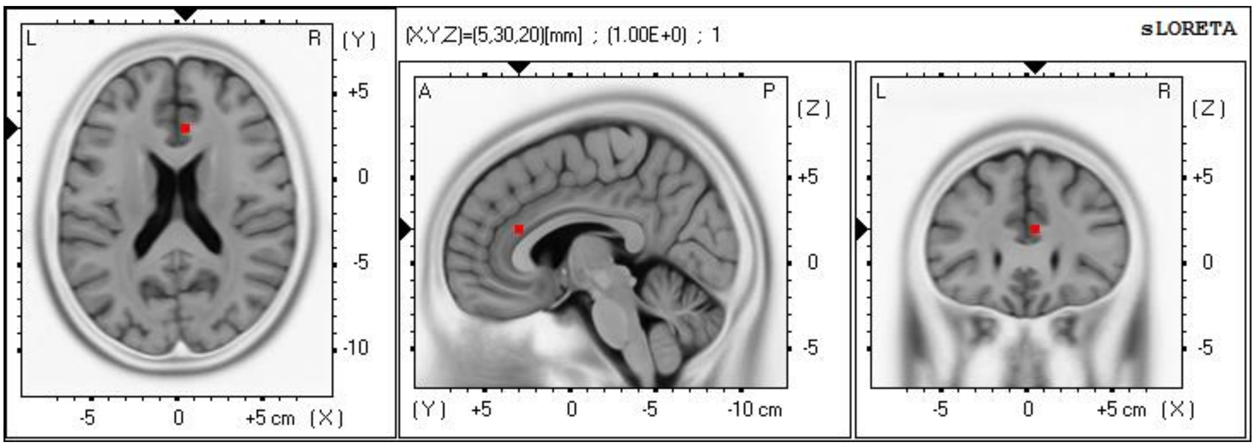
Appendix C

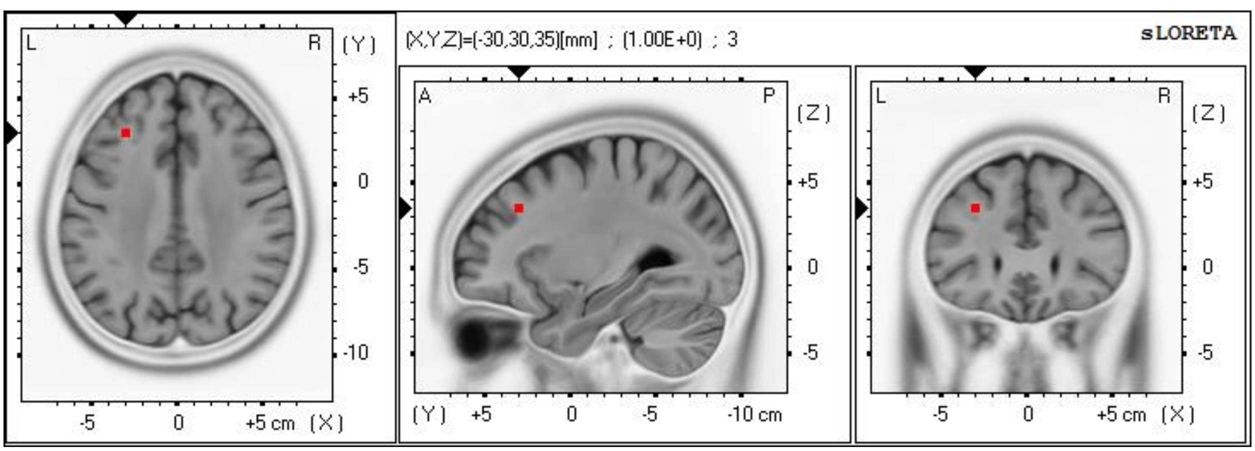
Regions of Interest Seeds

Experiment 2

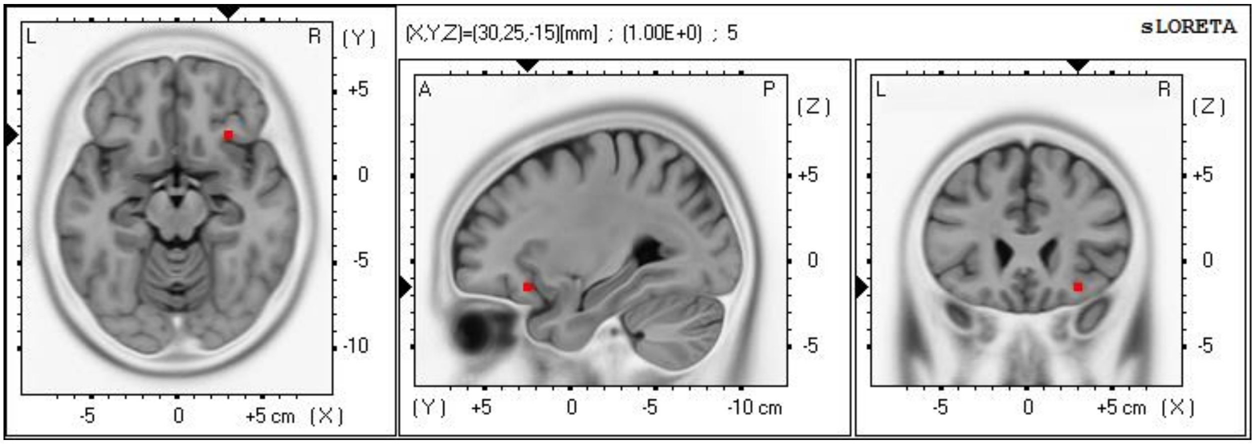
The single voxel and its nearest neighbor, where CSD was measured is represented as the red point in all images produced by sLORETA below.

Privacy Risk – Right BA 32 and Left BA 9, respectively

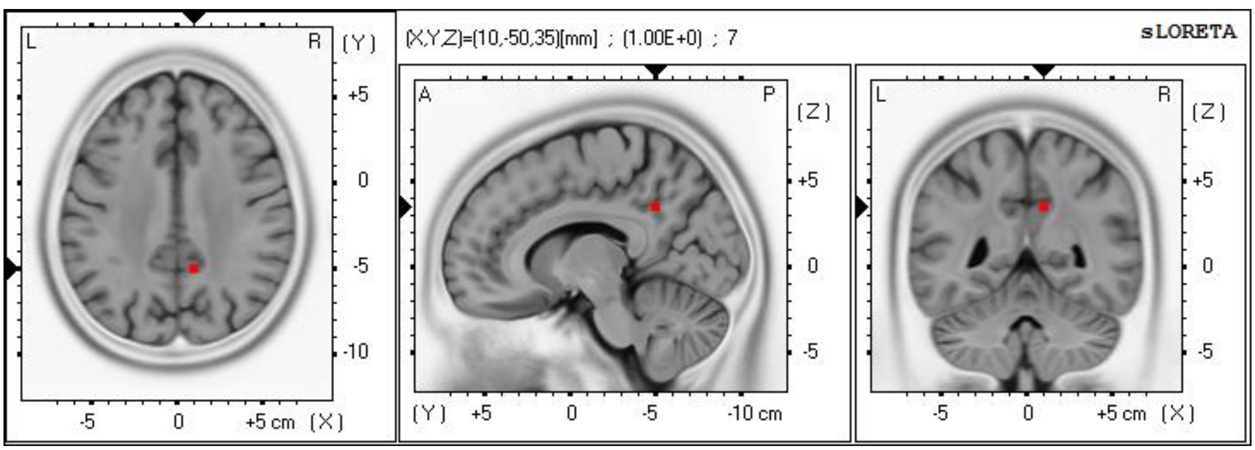


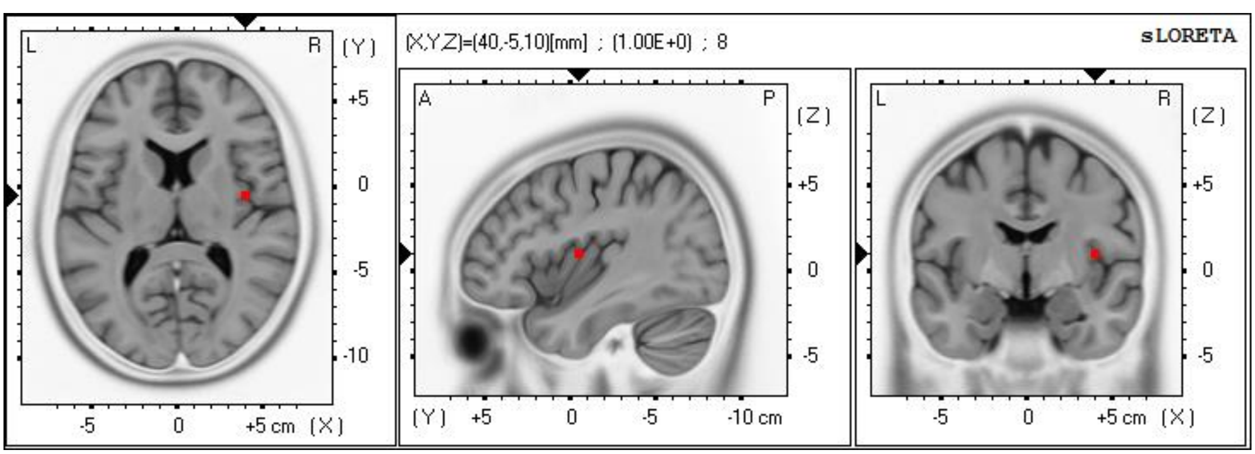


Trust – Right BA 47

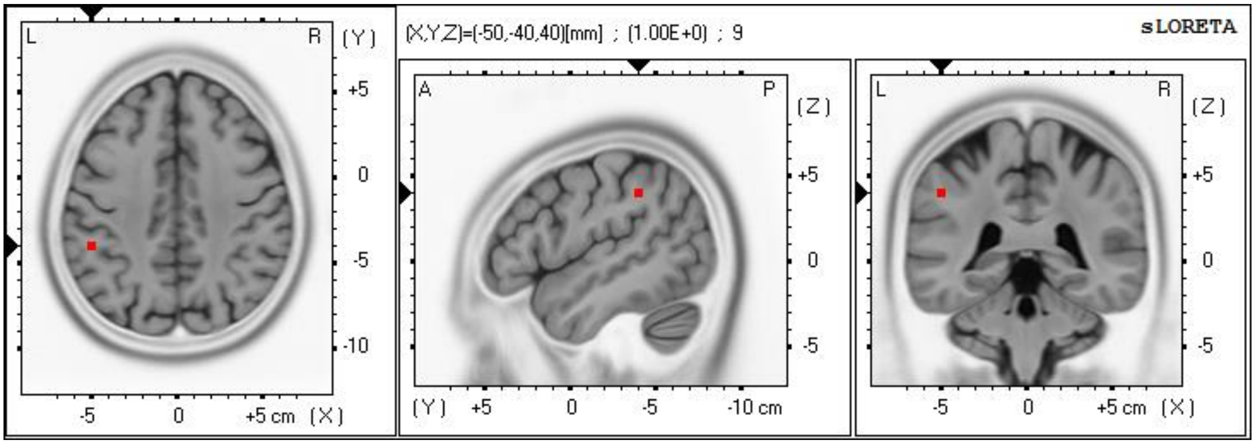


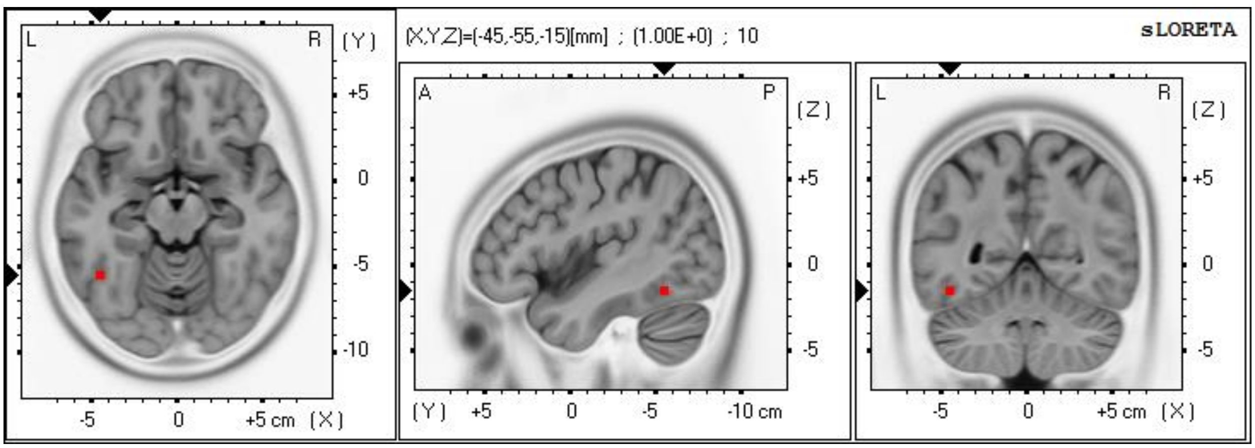
Distrust – Right BA 31 and BA 13, respectively





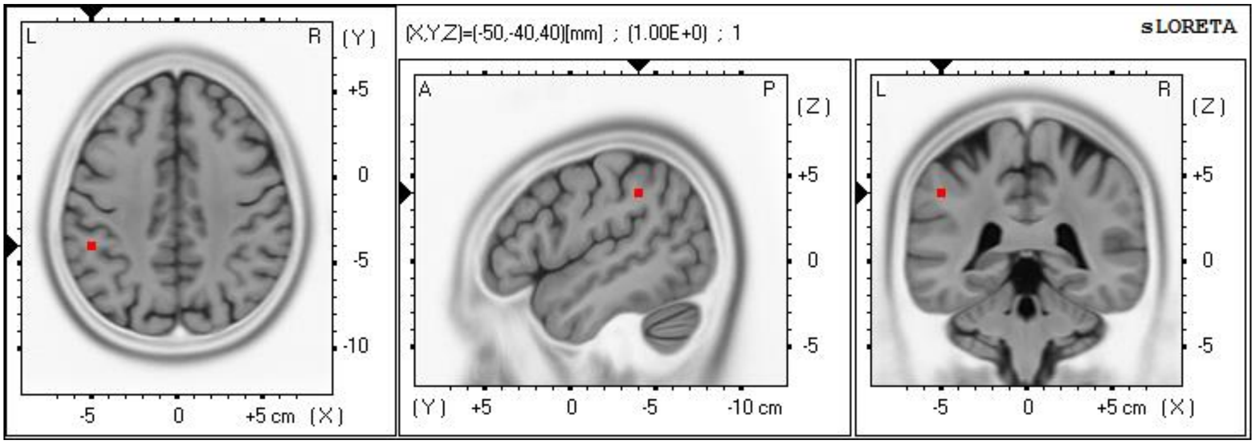
Personal Interest – Left BA 40 and 37, respectively

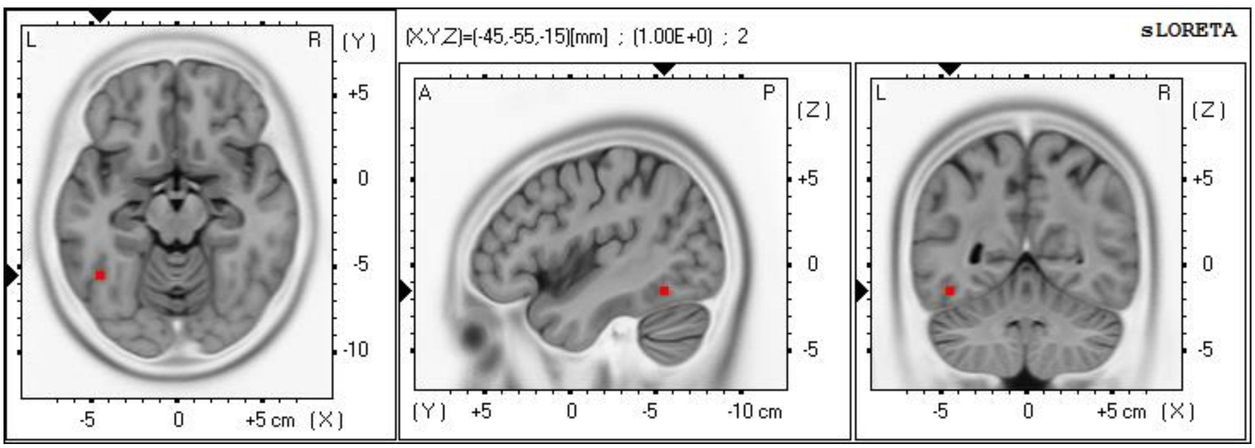




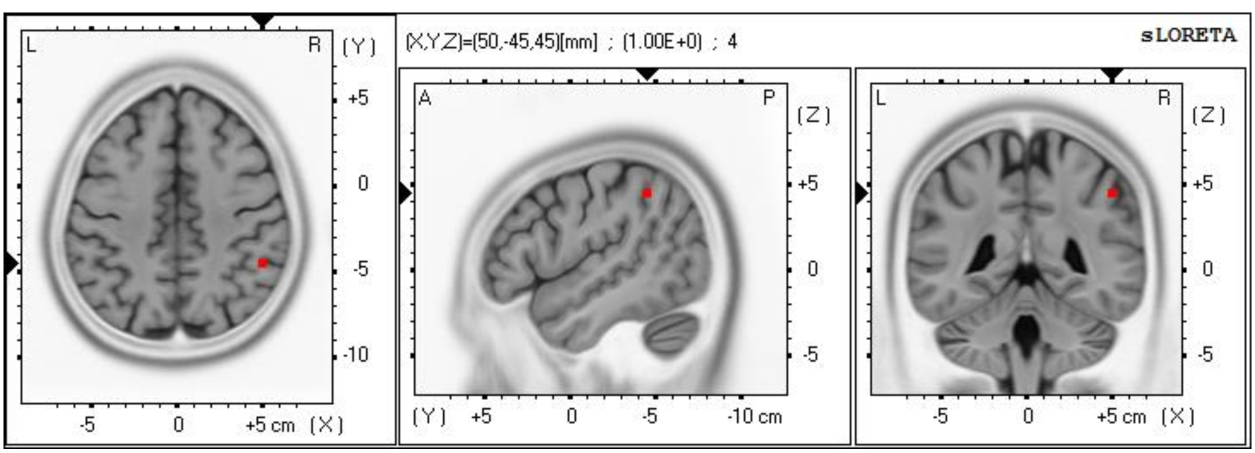
Experiment 3

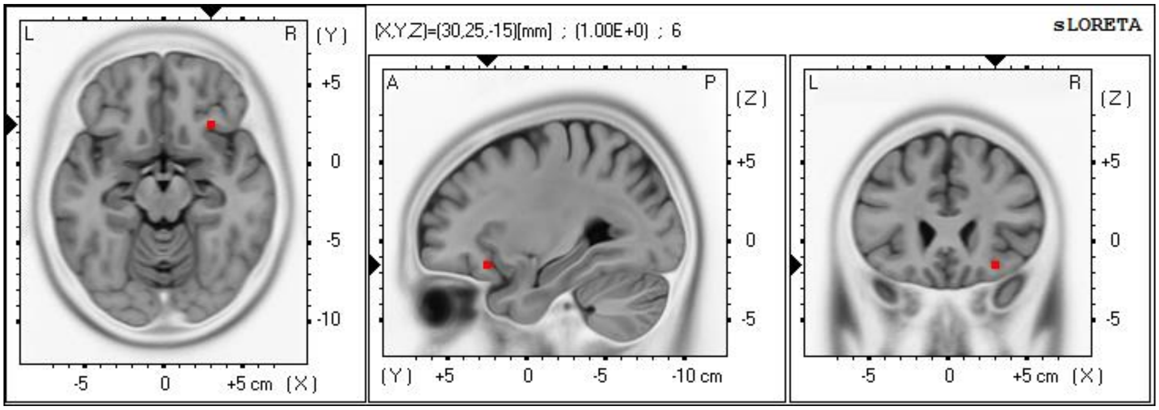
Personal Interest





Uncertainty – Right BA 40 and Right BA 47, respectively




(X,Y,Z)=(30,25,-15)[mm] ; (1.00E+0) ; 6
sLORETA
L
R
(Y)
+5
0
-5
-10
-5
0
+5 cm (X)
A
P
(Z)
+5
0
-5
(Y) +5
0
-5
-10 cm
L
R
(Z)
+5
0
-5
-5
0
+5 cm (X)

References

Acquisti, A. (2004). Privacy in electronic commerce and the economics of immediate gratification. *Proceedings of the 5th ACM Electronic Commerce Conference*, 21-29.

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security & Privacy, 3*(1), 26-33.

Acquisti, A., & Varian, H. R. (2005). Conditioning prices on purchase history. *Marketing Science, 24*(3), 367-381.

Allman, J. M., Hakeem, A., Erwin, J. M., Nimchinsky, E., & Hof, P. (2001). The anterior cingulate cortex: The evolution of an interface between emotion and cognition. *Annals of New York Academy of Science, 953*, 107-117.

Alderman, E., & Kennedy, C. (1997). *The right to privacy*. Vintage Books, New York.

Altman, I. (1975). *The environment and social behavior: Privacy personal space, territory, and crowding.* Brooks/Cole Publishing, Monterey, CA.

Anderson, C. L., & Agarwal, R. (2011). The digitization of healthcare: Boundary risks, emotion, and consumer willingness to disclose personal health information. *Information Systems Research, 22*(3), 469-490.

Angst, C. M., & 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), 339-370.

Andrade, E. B., Kaltcheva, V., & Weitz, B. (2002). Self-disclosure on the web: The impact of privacy policy, reward, and brand reputation. In *Advances in Consumer Research,* Brionarczyk, S. M., & Nakamoto, K. (eds.), Association for Consumer Research, Valdosta, GA, 350-353.

Awad, N. F., & 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), 13-28.

Ba, S. & Pavlou, P. A. (2002). Evidence of the effect of trust in electronic markets: Price premiums and buyer behavior. *MIS Quarterly, 26*(3), 243-267.

Bansal, G., Zahedi, F. M., & Gefen, D. (2008). The moderating influence of privacy concern on the efficacy of privacy assurance mechanisms for building trust : A multiple-context investigation. *Proceedings of 29th International Conference on Information Systems,* 14-17.

Bansal, G., Zahedi, F. M., & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems*, *49*, 138-150.

Belanger, F., & Crossler, R. E. (2011). Privacy in the digital age : A review of information privacy research in information systems. *MIS Quarterly, 35*(4), 1017-1041.

Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: The role of privacy, security, and site attributes. *Journal of Strategic Information Systems, 11*, 245 -270.

Belanger, F., & Xu, H. (2015). The role of information systems research in shaping the future of information privacy. *Information Systems Journal, 25*(6), 573-578.

Beuregard, M., Levesque, J., & Bourgouin, P. (2001). Neural correlates of conscious self-regulation of emotion. *Journal of Neuroscience, 21*(18), RC165.

Bench, C. J., Frith, C. D., Graspy, P. M., Friston, K. J., Paulesu, E., Frackowiak, R. S., & Dolan, R. J. (1993). Investigations of the functional anatomy of attention using the Stroop test. *Neuropsychologia, 31*(9), 907-922.

Bishop, L. S., Holmes, B. J., & Kelley, C. M. (2005). National consumer health privacy survey 2005. California HealthCare Foundation, Oakland, CA.

Brookshire, G., & Casasanto, D. (2012). Motivation and motor control: Hemispheric specialization for approach motivation reverses with handedness. *PLoS ONE, 7*(4), 1-5.

Brown, J. W., & Braver, T. S. (2007). Risk prediction and aversion by anterior cingulate cortex. *Cognitive, Affective, & Behavioural Neuroscience, 7*(4), 266-277.

Brunet, E., Sarfati, Y., Hardy-Bayle, M. C., & Decety, J. (2000). A PET investigation of the attribution of intentions with a nonverbal task. *Neuroimage, 11*(2), 157-166.

Bush, G., Vogt, B. A., Holmes, J., Dale, A. M., Greve, D., Jenike, M. A., & Rosen, B. R. (2001). Dorsal anterior cingular cortex: A role in reward-based decision making. *Proceedings of the National Academy of Sciences of the United States of America, 99*(1), 523-528.

Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., & Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems, 25*(6), 599-616.

Cabeza, R., & Nyberg, L. (2000). Imaging condition II: An empirical review of 275 PET and fMRI studies. *Journal of Cognitive Neuroscience, 12*(1), 1-47.

Cannon, R. L. (2009). *Functional connectivity of EEG LORETA in cortical core components of the self and the default network (DNt) of the brain* (Unpublished doctoral dissertation). University of Tennessee, Knoxville.

Cannon, R. L. (2012). *Low resolution electromagnetic tomography (LORETA) basic concepts and clinical applications.* USA: BMED Press.

Cannon, R. L., Congedo, M., Lubar, J., & Hutchens, T. (2009). Differentiating at network of executive attention: LORETA neurofeedback in anterior cingulate and dorsolateral prefrontal cortices. *International Journal of Neuroscience, 119*(3), 404-441.

Cannon, R. L., Sokhadze, E., Lubar, J., & Baldwin, D. (2008). LORETA neurofeedback for addiction and the possible neurophysiology of psychological processes influenced: A case study and region of interest analysis of LORETA neurofeedback in right anterior cingulate cortex. *Journal of Neurotherapy, 12*(4), 227-241.

Caudill, E. M., & Murphy, P. E. (2000). Consumer online privacy: Legal and ethical issues. *Journal of Public Policy & Marketing, 19*(1), 7-19.

Chellappa, R. K. (2008). Consumers' trust in electronic commerce transactions: The role of perceived privacy and perceived security. Unpublished Paper, Emory University, Atlanta, GA.

Clarke, R. (1999). Internet privacy concerns confirm the case for intervention. *Communications of the ACM, 42*(2), 60-67.

Cook, T. D., & Campbell, D. T. (1979). *Quasi-experimentation: Design and analysis issues for field settings*. Boston: Houghton Mifflin.

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

Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues, 59*(2), 323-342.

Culnan, M. J. (1993). "How did they get my name?" An exploratory investigation of consumer attitudes toward secondary information use. *MIS Quarterly, 17*(3), 341-364.

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

Davidson, R. J. (2002). Anxiety and affective style: role of prefrontal cortex and amygdala. *Biological Psychiatry, 51*(1), 68-80.

Davidson, R. J., Coe, C. C., Dolski, I., & Donzella, B. (1999). Individual differences in prefrontal activation asymmetry predict natural killer cell activity at rest and in response to challenge. *Brain Behavior and Immunity, 13*(2), 93-108.

Deegan, J. Jr. (1978). On the occurrence of standardized regression coefficients greater than one. *Educational and Psychological Measurement, 38*(4), 873-888.

DeGeorge, R. T. (2006). *The ethics of information technology and business.* Oxford: Blackwell Publishing Ltd.

Demos, J. N. (2005). *Getting started with neurofeedback.* New York: W.W. Norton & Company, Inc.

Deppe, M., Schwindt, W., Kugal, H., Plassmann, H., & Kenning, P. (2005). Nonlinear responses within the medial prefrontal cortex reveal when specific implicit information influences economic decision making. *Journal of Neuroimaging, 15*(2), 171-182.

Devinsky, O., Morrell, M. J., & Vogt, B. A. (1995). Contributions of anterior cingulate cortex to behaviour. *Brain 118*, 279-306.

di Michele, F., Prichep, L., John, E. R., & Chabot, R. J. (2005). The neurophysiology of attention-deficit/hyperactivity disorder. *International Journal of Psychophysiology, 58*, 81-93.

Dimoka, A. (2010). What does the brain tell us about trust and distrust? Evidence from a functional neuroimaging study. *MIS Quarterly, 34*(2), 373-396.

Dimoka, A. (2012). How to conduct a functional magnetic resonance (fMRI) study in social science research. *MIS Quarterly, 46*(3), 811-840.

Dimoka, A., Pavlou, P. A., & Davis, F.D. (2007). NeuroIS: The potential of cognitive neuroscience for information systems research. *28th International Conference of Information Systems, Montreal*, 1-20.

Dimoka, A., Pavlou, P. A., & Davis, F. D. (2011). NeuroIS: The potential of cognitive neuroscience for information systems research. *Information Systems Research, 22*(4), 687-702.

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., & Colautti, C. (2006). Privacy calculus model in e-commerce - A study of Italy and the United States. *European Journal of Information Systems, 15*, 389-402.

Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents - Measurement validity and regression model. *Behavioural Information Technology, 23*(6), 413-422.

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

Dinev, T., Xu, H., & Smith, H. J. (2009). Information privacy values, beliefs, and attitudes: An empirical analysis of web 2.0 privacy. *Proceedings of the 42nd Hawaii International Conference on Systems Sciences*, 1-10.

Dupont, D. (2002). Investigating temporal pole function by functional imaging. *Epileptic Disorder, 4*, 17-22.

Emotiv Inc. (2016). Emotiv EPOC+. *Retrieved from http://i1.wp.com/emotiv.com/wp-content/uploads/2016/02/emotiv_epoc_600.png?w=600*.

Ernst, M., Nelson, E. E., McClure, E. B., Monk, C. S., Munson, S., Eshel, S,..., Pine, D. S. (2004). Choice selection and reward anticipation: An fMRI study. *Neuropsychologia, 42*(12), 1585-1597.

Federal Trade Commission. (1998). *Privacy online: A report to congress,* (June). Washington, DC: Federal Trade Commission.

Grech, R., Cassar, T., Muscat, J., Camilleri, K. P., Fabri, S. G., Zervakis, M., Xanthopoulos, P., Sakkalis, V., & Vanrumste, B. (2008). Review on solving the inverse problem in EEG source analysis. *Journal of NeuroEngineering and Rehabilitation, 5*(25), 1-33.

Greenaway, K. E., Chan, Y. E., & Crossler, R. E. (2015). Company information privacy orientation: A conceptual framework. *Information Systems Journal, 25*, 579-606.

Goldberg, S. (2010). *Clinical Neuroanatomy made ridiculously simple (4th eds.).* Miami: MedMaster, Inc.

Gut, M., Urbanik, A., Forsberg, L., Binder, M., Rymarczyk, K., Sobiecka, B., Kozub, J., & Grabowska, A. (2007). Brain correlates of right-handedness. *Acta Neurobiologiae Experimentalis, 67*(1), 43-51.

Guyton, A. C., & Hall, J. E. (2001). *Pocket companion to textbook of medical physiology* (10th eds.). Philadelphia: W. B. Saunders Company.

Hanaway, J., Woosley, W. A., Gado, M. H., & Melville, R. P., Jr. (1998). *The brain atlas: A visual guide to the human central nervous system.* Bethesda: Fitzgerald Science Press.

Harris Interactive, & Westin, A. F. (2001). *The Harris Poll: #49 (2001).* Harris Interactive, Rochester, NY.

Hellige, J. B. (1993). *Hemispheric asymmetry.* Cambridge, MA: Harvard University Press.

Hollander, E., Pallanti, S, Baldini, R. N, Sood, E., Baker, B. R., & Buchsbaum, M. S. (2005). Imaging monetary reward in pathological gamblers. *World Journal of Biological Psychiatry, 6*(2), 113-120.

Hsu, C. –W. (2006). Privacy concerns, privacy practices and web site categories. *Online Information Review, 30*(5), 569-585.

Hui, K. –L., Teo, H. H., & Lee, S. –Y., T. (2007). The value of privacy assurance: An exploratory field experiment. *MIS Quarterly, 31*(1), 19-33.

Hong, W., & Thong, J. Y. L. (2013). Internet privacy concerns: An integrated conceptualization and four empirical studies. *MIS Quarterly 37*(1), 275-298.

Huettel, S., & Song, A. (2008). *Functional magnetic resonance imaging* (2^{nd} ed.). Sunderland, Massachusetts: Sinauer Associates.

Jahanashi, M., Dirnberger, G., Fuller, R., & Frith, C. D. (2000). The role of the dorsolateral prefrontal cortex in random number generation: A study with positron emission tomography. *Neuroimage, 12*(6), 713-725.

Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica, 47*(2), 263-292.

Kalgotra, P., Sharda, R., & Chakraborty, G. (2014). Association mining of the brain data: An EEG study. *In SAS Global Forum Proceedings*.

Kehr, F., Wentzel, D., & Kowatsch, T. (2014). Privacy paradox revised: Pre-existing attitudes, psychological ownership, and actual disclosure. *Proceedings of 35^{th} International Conference on Information Systems,* 1-12.

Kirimoto, H., Ogata, K., Onishi, H., Oyama, M., Goto, Y., & Tobimatsu, S. (2010). Transcranial direct current stimulation over the motor association cortex induces plastic changes in ipsilateral primary motor and somatosensory cortices. *Clinical Neurophysiology, 122*, 777-783.

Knauff, M., Mulack, T., Kassubek, J., Salih, H. R., & Greenlee, M. W. (2002). Spatial imagery in deductive reasoning: A functional MRI study. *Cognitive Brain Research, 13*(2), 203-212.

Knutson, B., Adams, C. M., Fong, G. W., & Hommer, D. (2001). Anticipation of increasing monetary reward selectively recruits nucleus accumbens. *The Journal of Neuroscience, 21*, 1-5.

Kraine, A., Wilson, A. M., Arbuckle, R., Castellanos, F. X., & Milham, M. P. (2006). Distinct neural mechanisms of risk and ambiguity: A meta-analysis of decision-making. *Neuroimaging*, *32*(1), 477-484.

Kringelbach, M. L. (2005). The human orbitofrontal cortex: Linking reward to hedonic experience. *Nature Reviews Neuroscience*, *6*, 691-702.

Kringelbach, M. L., & Rolls, E. T. (2004). The functional neuroanatomy of the human orbitofrontal cortex: Evidence from neuroimaging and neuropsychology. *Progress in Neurobiology*, *72*, 341-372.

Lacadie, C. M., Fulbright, R. K., Constable, R. T., and Papademetris, X. (2008). More accurate Talairach coordinates for neuroimaging using nonlinear registration. *Neuroimage*, *42*(2), 717-725.

Lane, R. D., Reiman, E. M., Bradley, M. M., Lang, P. J., Ahem, G. L., Davidson, R. J., & Schwartz, G. E. (1997). Neuroanatomical correlates of pleasant and unpleasant emotion. *Neuropsychologia, 35*(11), 1437-1444.

Lang, E. W., Tome, A. M., Keck, I. R., Gorriz-Saez, J. M., & Puntonet, C. G. (2012). Brain connectivity analysis: A short survey. *Computational Intelligence and Neuroscience*, *2012*(412512), 1-21.

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: Multidimensional development theory. *Journal of Social Issues*, *33*(3), 22-42.

Leube, D. T., Erb, M., Grodd, W., Bartels, M., & Kircher, T. T. (2001). Differential activation in parahippocampal and prefrontal cortex during word and face encoding tasks. *Neuroreport*, *12*(12), 2773-2777.

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*, 434-445.

Li, X. B., & Sarker, S. (2006). Privacy protection in data mining: A perturbation approach for categorical data. *Information Systems Research*, *17*(3), 254-270.

Libenson, M. H. (2010). *Practical approach to electroencephalography.* Philadelphia: Saunders Elsevier.

Lin, Y., & Wu, H. –Y. (2008). Information privacy concerns, government involvement, and corporate policies in the consumer relationship management context. *Journal of Global Business and Technology, 4*(1), 79-91.

Liu, C., & Arnett, K. P. (2002). Raising a red flag on global WWW privacy policies. *The Journal of Computer Information Systems, 43*(1), 117-127.

Liu, C., Marchewka, J. T., Lu, J., & Yu, C. –S. (2005). Beyond concern – a privacy-trust-behavioral intention model of electronic commerce. *Information & Management,42*, 289-304.

Luria, A. R. (1966). *Higher Cortical Functions in Man (2nd Edition).* New York: Basic Books Inc.

Madden, M., Fox, S., Smith, A., & Vitak, J. (2007). Digital footprints: Online identity management and search in the age of transparency. *PEW Research Center Publications*.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research, 15*(4), 336-355.

Margulis, S. T. (1977). Conceptions of privacy: Current status and next steps. *Journal of Social Issues, 33*(3), 5-21.

Mason, M. L. (1986). Four ethical issues of the information age. *MIS Quarterly, 10*(1), 5-12.

Massar, S. A. A., Rossi, V., Schutter, D. J. L. G., & Kenemans, J. L. (2012). Baseline EEG theta/beta ratio and punishment sensitivity as biomarkers for feedback-related negativity (FRN) and risk-taking. *Clinical Neurophysiology, 123*, 1958-1965.

Matthews, S. C., Simmons, A. N., Lane, S. D., & Paulus, M. P. (2004). Selective activation of the nucleus accumbens during risk-taking decision making. *Neuroreport, 15*(13), 2123-2127.

McCaslin, A. F., Chen, B. R., Radosevich, A. J., Cauli, B., & Hillman, E. M. (2010). In vivo 3D morphology of astrocyte-vasculature interactions in the somatosensory cortex: Implications for neurovascular coupling. *Journal of Cerebral Blood Flow and Metabolism, 31*, 795-806.

Micceri, T. (1989). The unicorn, the normal curve, and other improbably creatures. *Psychological Bulletin, 105*(1), 156-166.

Milne, G. R., & Boza, M., -E. (1999). Trust and concern in consumers' perception of marketing information management practices. *Journal of Interactive Marketing, 13*(1), 5-24.

Miyazaki, A., & Krishnamurthy, S. (2002). Internet seals of approval: Effects on online privacy policies and consumer perceptions. *Journal of Consumer Affairs, 36*(1), 28-49.

Mohammed, Z. A., & Tejay, G. P. (2015). The role of cognitive disposition in deconstructing the privacy paradox: A neuroscience study. *In Proceedings of the 21st Americas Conference on Information Systems*.

Moores, T. (2005). Do consumers understand the role of privacy seals in e-commerce? *Communications of the ACM, 48*(3), 86-91.

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information intentions versus behavior. *The Journal of Consumer Affairs, 41*, 100-126.

Nichols, T. E., & Holmes, A. P. (2001). Nonparametric permutation tests for functional neuroimaging: A primer with examples. *Human Brain Mapping, 15*, 1-25.

O'Brien, R. M. (2007). A caution regarding rules of thumb for variance inflation factors. *Quality & Quantity, 41*, 673-690.

Olofsson, J. K., Nordin, S., Sequeira, H., & Polich, J. (2008). Affective picture processing: An integrative review of ERP findings. *Biological Psychology, 77*(3), 247-265.

Osbourne, J. W. (2002). Notes on the use of data transformations. *Practical Assessment, Research & Evaluation, 8*(6), 1-7.

Osbourne, J. W. (2010). Improving your data transformations: Applying the Box-Cox transformation. *Practical Assessment, Research & Evaluations*, *15*(12), 1-9.

Pascual-Marqui, R., D. (1999). Review of methods for solving EEG inverse problem. *International journal of bioelectromagnetism, 1*(1), 75-86.

Pascual-Marqui, R. D. (2002). Standardized low resolution brain electromagnetic tomography (sLORETA): Technical details. *Methods & Findings in Experimental & Clinical Pharmacology, 24*(Supp. D), 5-12.

Pascual-Marqui, R. D., Esslen, M., Kochi, K., & Lehmann, D. (2002). Functional imaging with low resolution brain electromagnetic tomography (LORETA): Review, new comparisons, and new validation. *Japanese Journal of Clinical Neurophysiology, 30*, 81-90.

Paulus, M. P. & Frank, L. R. (2003). Ventromedial prefrontal cortex activation is critical for preference judgements. *Neuroreport, 14*(10), 1311-1315.

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

Pavlou, P. A. & Dimoka, A. (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), 391-412.

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

Pease, B., & Pease, A. (2000). *Why men don't listen and women can't read maps*. New York : Broadway.

Peter, J. P., & Tarpey, S. L. X. (1997). A comparative analysis of three consumer decision strategies. *Journal of Consumer Research, 2*(1).

Pizzagalli, D. A., Oakes, T. R., & Davidson, R. J. (2003). Coupling of theta activity and glucose metabolism in the human rostral anterior cingulate cortex: An EEG/PET study of normal and depressed subjects. *Psychophysiology, 40*(6), 939-949.

Phelps, E. A. (2006). Emotion and cognition : insights from studies of the human amygdala. *Annual Review of Psychology, 57*, 27-53.

Phelps, E. A., O'Connor, K. J., Gatenby, J. C., Gore, J. C., Grillon, C., & Davis, M. (2001). Activation of the left amygdala to a cognitive representation of fear. *Natural Neuroscience, 4*(4), 437-441.

Pochon, J., Levy, R., Poline, J., Crozier, S., Lehericy, S., Pillon, B.,…Dubois, B. (2001). The role of dorsolateral prefrontal cortex in the preparation of forthcoming actions: An fMRI study. *Cerebral Cortex, 11*(3), 260-266.

Poldrack, R. A. (2006). Can cognitive processes be inferred from neuroimaging data?. *Trends in Cognitive Sciences, 10*(2), 59-63.

Poldrack, R. A. (2007). Region of interest analysis for fMRI. *Social Cognitive Affective Neuroscience, 2,* 67-70.

Posner, R. A. (1984). An economic theory of privacy. In F. Schoeman (ed.), *Philosophical dimensions of privacy : An anthology* (pp. 333-345). New York : Cambridge Press University.

Posner, M. I., & Rothbart, M. K. (1998). Attention, self-regulation, and consciousness. *Philosophical Transactions of the Royal Society B: Biological Sciences*, *353*(1377), 1915–1927.

Reinders, A. A., Glascher, J., de Jong, J. R., Willemsen, A. T., den Boer, J. A., & Buchel, C. (2006). Detecting fearful and neutral faces: BOLD latency differences in amygdala-hippocampal junction. *Neuroimage, 33*(2), 806-814.

Rektor, I, Rektorova, I, Mikl, M., Brazdil, M., & Krupa, P. (2006). An event-related fMRI study of self-paced alphabetically ordered writing of single letters. *Experimental Brain Research, 173*(1), 79-85.

Richardson, M. P., Strange, B. A., & Dolan, R. J. (2004). Encoding of emotional memories depends on amygdala and hippocampus and their interactions. *Natural Neuroscience, 7*(3), 278-285.

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), 243-264.

Rifon, N. J., LaRose, R., & Choi, S. M. (2005). Your privacy is sealed: Effects of web privacy seals on trust and personal disclosures. *Journal of Consumer Affairs, 39*(2), 339-362.

Rogers, R. D., Owen, A. M., Middleton, H. C., Williams, E. J., Pickard, J. D., Sahakian, B. J., & Robbins, T. W. (1999). Choosing between small, likely rewards and large, unlikely rewards activates inferior and orbital prefrontal cortex. *Journal of Neuroscience*, *19*(20), 9029-9038.

Rose, E. A. (2006). An examination of the concern for information privacy in the New Zealand regulatory context. *Information & Management*, *43*, 322-335.

Sawamoto, N., Honda, M., Okada, T., Hanakawa, T., Kanda, M., Fukuyama, H.,…Shibasaki, H. (2000). Expectation of pain enhances responses to nonpainful somatosensory stimulation in the anterior cingulate cortex and parietal operculum/posterior insula: An event-related functional magnetic resonance imaging study. *Journal of Neuroscience, 20*(19), 7438-7445.

Scherg, M. (1990). Fundamentals of dipole source potential analysis. *Auditory evoked magnetic fields and electric potentials, 6*, 40-69.

Schoeman, F. (1984). *Philosophical dimensions of privacy: An anthology.* Cambridge University Press, New York.

Schonwald, L. I., & Muller, M. M. (2014). Slow biasing of processing resources in early visual cortex is preceded by emotional cue extraction in emotion-attention competition. *Human Brain Mapping*, *35*(4), 1477-1490.

Schwaig, K. S., Kane, G. C., & Storey, V. C. (2006). Compliance to the fair information practices: How are the fortune 500 handling online privacy disclosures?. *Information & Management*, *43,* 805-820.

Seeley, C. J., Smith, C. T., MacDonald, K. J., & Beninger, R. J. (2016). Ventromedial prefrontal theta activity during rapid eye movement sleep is associated with improved decision-making on the Iowa gambling task. *Behavioural Neuroscience, 130*(3), 271-280.

Sekaren, U., & Bougie, R. (2013). *Research methods for business*. United Kingdom: John Wiley & Sons Ltd.

Sim, I., Liginlal, D., & Khansa, L. (2012). Information privacy situation awareness: Construct and validation. *Journal of Computer Information Systems, 53*(1), 57-64.

Skinner, G., Han, S., & Chang, E. (2006). An information privacy taxonomy for collaborative environments. *Information Management & Computer Security, 14*(4), 382-394.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly 35*(4), 989-1015.

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

Snell, R. S. (2010). *Clinical neuroanatomy, 7th Edition.* Philadelphia: Lippincott Williams & Wilkens.

Soderfeldt, B., Ingvar, M., Ronnberg, J., Eriksson, L., Serrander, M., & Stone-Elander, S. (1997). Signed and spoken language perception studied by positron emission tomography. *Neurology, 49*(1), 82-87.

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennyslvania Law Review, 15*(3), 477-564.

Stefanatos, G. A., Joe, W. Q., Aguirre, G. K., Detre, J. A., & Wetmore, G. (2008). Activation of human auditory cortex during speech perception: Effects of monaural, bunaural, and dichotic presentation. *Neuropsychologia, 46*(1), 301-315.

Stephan, K. M., Fink, G. R., Passingham, R. E., Silbersweig, D., Ceballos-Baumann, A. O., Frith, C. D., & Frackowiak, R. S. (1995). Functional anatomy of the mental representation of upper extremity movements in healthy subjects. *Journal of Neurophysiology, 73*(1), 373-386.

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

Stone, E. F., & Stone, D. L. (1990). Privacy in organizations: Theoretical issues, research findings, and protection mechanisms. *Research in Personnel and Human Resources Management, 8*(3), 349-411.

Straub, T., & Miltner, W. H. (2011). Attention to aversive emotion and specific activation of the right insula and right somatosensory cortex. *Neuroimage, 54*(3), 2534-2538.

Sur, S., & Sinha, V. (2009). Event-related potential: An overview. *Industrial Psychiatry Journal*, *18*(1), 70-73.

Sutanto, J., Palme, E., Tan, C. -H., & Phang, C. W. (2013). Addressing the personalization-privacy paradox: An empirical assessment from a field experiment on smartphone users. *MIS Quarterly, 37*(4), 1141-1164.

Talairach, J. T. P. (1988). *Co-planar stereoaxic atlas of the human brain.* New York: Theme Medical Publishers.

Tanaka, K. (1997). Mechanisms of visual object recognition: Monkey and human studies. *Current Opinion on Neurobiology, 7*(4), 523-529.

Teplan, M. (2002). Fundamentals of EEG measurements. *Measurement Science Review, 2*(2), 1-11.

The Privacy Act of 1974 (1974). Retrieved from: http://www.justice.gov/opcl/privacy-act-1974.

US Censor News. (2015). Quarterly retail ecommerce sales 1st quarter 2015. *Retrieved from: https://www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf.*

Van Slyke, C., Shim, J. T., Johnson, R., & Jiang, J. (2006). Concern for information privacy and online consumer purchasing. *Journal of the Association for Information Systems, 7*(6), 415-444.

Vance, A., Anderson, B. B., Kirwan, C. B., & Eargle, D. (2014). Using measures of risk perception to predict information security behaviour: Insights form electroencephalography (EEG). *Journal of the Association for Information Systems*, *15*, 679-722.

Vogt, B. A., Finch, D. M., & Olson, C. R. (1992). Functional heterogeneity in cingulate cortex: The anterior executive and posterior evaluative regions. *Cerebral Cortex, 2*(6), 435-443.

Volz, K. G., Schubotz, R. I., & von Cramon, D. Y. (2005). Variants of uncertainty in decision-making and their neural correlates. *Brain Research Bulletin, 67*(5), 403-412.

Warren, S. D., & Brandeis, D. L. (1980). The right to privacy. *Harvard Law Review, 4*(5), 193-220.

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

Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2008). Examining the formation of individual's information privacy concerns: Toward an integrative view. *Proceedings of the 29th Annual International Conference on Information System,* 1-16.

Xu, H., Teo, H. –H., Tan, B. C. Y., & Agarwal, R. (2005). Predicting the adoption of location-based services: The roles of trust and privacy risk. *Proceedings of 26th International Conference on Information Systems*, 897-910.

Xu, H., Teo, H. –H., Tan, B. C. Y., & 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), 135-173.

Xu, H., Teo, H. –H., Tan, B. C. Y., & Agarwal, R. (2012). Effects of self-protection, industry self-regulation, and government regulation on privacy concerns: A study of location-based services. *Information Systems Research*, *23*(4), 1342-1363.

Xu, Q., Shen, Q., Chen, P., Ma, Q., Sun, D., & Pan, Y. (2011). How an uncertain cue modulates subsequent monetary outcome evaluation: An ERP study. *Neuroscience Letters, 505*, 200-204.

Zhang, Z., Jiao, y. y., & Sun, Q. Q. (2011). Developmental maturation of excitation and inhibition balance in principal neurons across four layers of somatosensory cortex. *Neuroscience, 174*, 10-25.

Zimney, G. H. (1961). *Methods in Experimental Psychology.* New York: Ronald Press.

Zotev, V., Phillips, R., Yuan, H., Misaki, M., & Bodurka, J. (2014). Self-regulation of human brain activity using simultaneous real-time fMRI and EEG neurofeedback. *NeuroImage, 85*, 985-995.

Zotev, V., Yuan, H., Misaki, M., Phillips, R., Young, K. D., Feldner, M. T., & Bodurka, J. (2016). Correlation between amygdala BOLD activity and frontal EEG asymmetry during real-time fMRI neurofeedback training in patients with depression. *NeuroImage: Clinical, 11*, 224-238.

Zysset,S., Huber, O., Ferstl, E., & von Cramon, D. Y. (2002). The anterior frontomedian cortex and evaluative judgement: An fMRI study. *Neuroimage, 15*(4), 983-991.