Fall 2016

Perceived patient control over personal health information in the presence of context-specific concerns

Prabhashi A. Nanayakkara
Louisiana Tech University

PERCEIVED PATIENT CONTROL OVER PERSONAL HEALTH INFORMATION IN THE PRESENCE OF CONTEXT-SPECIFIC CONCERNS

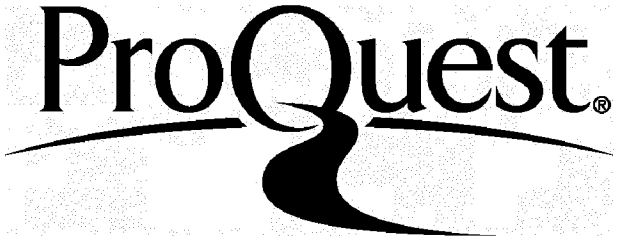
by

Prabhashi A.Nanayakkara, B.S., M.B.A.

A Dissertation Presented in Partial Fulfillment
of the Requirements for the Degree
Doctor of Business Administration

COLLEGE OF BUSINESS
LOUISIANA TECH UNIVERSITY

November 2016



LOUISIANA TECH UNIVERSITY

THE GRADUATE SCHOOL

August 8, 2016

Date

We hereby recommend that the dissertation prepared under our supervision by Prabhashi Nanayakkara

entitled Perceived Patient Control Over Personal Health Information in the Presence of Context-Specific Concerns

be accepted in partial fulfillment of the requirements for the Degree of Doctor of Business Administration

Dr. T. Selwyn Ellis Supervisor of Dissertation Research

Dr. T. Selwyn Ellis Head of Department

Computer Information Systems

Department

Recommendation concurred in:

Dr. T. Selwyn Ellis

Dr. James F. Courtney

Dr. Angela Kennedy

Advisory Committee

Approved:

Director of Graduate Studies, Dr. John Francis

Dean of the College, Dr. Christopher Martin

Approved:

Dean of the Graduate School, Dr. Sheryl Shoemaker

GS Form 13a
(6/07)

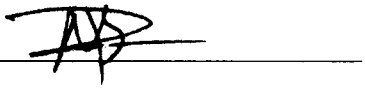
ABSTRACT

Information privacy issues have plagued the world of electronic media since its inception. This research focused mainly on factors that increase or decrease perceived patient control over personal health information (CTL) in the presence of context-specific concerns. Control agency theory was used for the paper's theoretical contributions. Personal and proxy control agencies acted as the independent variables, and context-specific concerns for information privacy (CFIP) were used as the moderator between proxy control agency, healthcare provider, and CTL. Demographic data and three control variables—the desire for information control, privacy experience, and trust propensity—were also included in the model to gauge the contribution to CTL from external factors. Only personal control agency and desire for information control were found to impact CTL.

APPROVAL FOR SCHOLARLY DISSEMINATION

The author grants to the Prescott Memorial Library of Louisiana Tech University the right to reproduce, by appropriate methods, upon request, any or all portions of this Dissertation. It is understood that "proper request" consists of the agreement, on the part of the requesting party, that said reproduction is for his personal use and that subsequent reproduction will not occur without written approval of the author of this Dissertation. Further, any portions of the Dissertation used in books, papers, and other works must be appropriately referenced to this Dissertation.

Finally, the author of this Dissertation reserves the right to publish freely, in the literature, at any time, any or all portions of this Dissertation.

Author 

Date 08/08/2016

GS Form 14
(5/03)

TABLE OF CONTENTS

ABSTRACT iii

LIST OF TABLES xii

LIST OF FIGURES xiv

CHAPTER ONE INTRODUCTION 1

CHAPTER TWO LITERATURE REVIEW 7

General Privacy Definitions 7

General Privacy 7

Privacy as a Commodity 10

Cognate-Based Definitions 11

General Privacy as a Control 11

General vs. Context-Specific Concerns for Information Privacy 12

Information Privacy 13

Health-Related Privacy 15

Control Agency Theory 18

Privacy Concerns as a Measurable Proxy for Privacy 20

Perceived Patient Control over Personal Health Information (CTL) 21

The Impact of Control Agencies on Perceived Patient Control over Personal Health Information (CTL) in the Presence of Context-Specific Concerns 22

Hypotheses Development 23

Personal Control Agency (PCA) 23

Proxy Control Agency (PRCA) 23

Organizational Proxy Control Agency (OPRCA): Healthcare Provider (HCP) 23

The Impact of Context-Specific Privacy Concerns (CFIP) on Healthcare Provider (HCP) 25

Organizational Proxy Control Agency (OPRCA): Government 25

Control Variables (Rival Explanations) 26

CHAPTER THREE RESEARCH METHODOLOGY 28

Constructs and Variables 28

Personal Control Agency 29

Proxy Control Agency 29

Perceived Patient Control over Personal Health Information (CTL) 30

Context-Specific Concerns for Information Privacy (CFIP) 30

Control Variables 30

Model and Instrument Design 31

Preliminary Testing 32

Primary Study 32

CHAPTER FOUR DATA ANALYSIS AND RESULTS 35

Data Cleansing and Assumption Testing 35

Measurement Validation 36

Hypotheses Testing: Path Coefficients for Structural Model 40

CHAPTER FIVE CONTRIBUTIONS AND LIMITATIONS 45

Contributions 45

Contributions to Patients and Practitioners....45

Contributions to Academia....47

Limitations and Future Recommendations....47

APPENDIX A SURVEY INSTRUMENT....49

APPENDIX B HUMAN USE APPROVAL FORM....54

REFERENCES....56

LIST OF TABLES

Table 3.1 *Construct Measurements* 31

Table 3.2 *Profile of the Participants* 33

Table 4.1 *Factor Analysis: Convergent and Discriminant Validity* 37

Table 4.2 *Cronbach's Alpha* 38

Table 4.3 *Average Variance Extracted* 38

Table 4.4 *Statistical Power Analysis* 39

Table 4.5 *Path Analysis* 41

Table 4.6 *Hypotheses Testing* 43

LIST OF FIGURES

Figure 2.1 *Research Model* 23

Figure 4.1 *The Main Effects Model* 39

Figure 4.2 *CFIP: Second-Order Formative Factor* 40

Figure 4.3 *Full Model* 42

CHAPTER ONE

INTRODUCTION

This chapter provides an overview of the complete study, which includes an exploration of privacy statistics, concepts, theories, research model and methods, contributions, and limitations.

Privacy is the right to exist without being exposed to select private or public interventions (Rachels, 1975). A person's ability to remove him- or herself from society on a short- or long-term basis has been noted as a state of general privacy (Westin, 1968). Warren and Brandeis (1890) defined the scope of privacy as "the safeguard of life and property over time." This scope extends to safeguarding an individual's immunity, spiritual beliefs, emotions, and intellectual properties (Warren and Brandeis, 1890). Warren and Brandeis also stated that, in some cases, privacy breaches often can lead to greater emotional agony and can be more detrimental than physical injury (1890). Prior literature has documented a plethora of detrimental effects-caused privacy violations.

Regardless of these detrimental effects, privacy violations have continued to increase. The Poneman Institute's "2015 Cost of Cyber Crime Study: Global" was conducted by interviewing 2,128 company personnel from 252 companies in seven countries and studying 1,928 total attacks. The study found that, in 2015, global data violations cost an average of $7.7 million, representing a 1.9% net increase from 2014

(Poneman, 2015). Of the countries studied, the U.S. had the highest cybercrime cost, totaling $15.5 million since 2013 (Poneman, 2015). After consulting 58 industries from both the public and private sector, The Poneman Institute's "2015 Cost of Cyber Crime Study: The United States" reported that the mean annual cost of data breaches in 2015 totaled $15 million, compared to $12.7 million in 2014. This $2.7 million difference amounted to a 19% increase in the mean value and contributed to an overall rise of 82% in cyber crimes over the last six years.

The Privacy Rights Clearinghouse's "Chronology of Data Breaches" report indicated there were 154 cyber-crimes in 2015, which led to about 153.5 million record breaches (Clearinghouse, 2015). The number of records breached increased by about 45% in 2015 compared to 2014 and included breaches in the business sector (financial, insurance services, and retail merchants), educational institutions, government, military, and healthcare (Clearinghouse, 2015). The types of breach types consisted of unintentional disclosures on the web, hacking or malware, payment card fraud, insider threats, physical loss, portable and stationary device theft, and unknown attacks (Clearinghouse, 2015). These findings illustrate the importance of information privacy and the costs involved when privacy is compromised.

In 2015, 17% of the breaches were healthcare data breaches, and the number of records compromised increased at a rate of about 45% from that of 2014 (Clearinghouse, 2015). According to Poneman, 10% of all breaches in 2015 were healthcare cybercrimes (Poneman, 2015). These analyses verify that healthcare privacy breaches have risen over the years.

Personal health information privacy is one of the most crucial and sensitive subjects for patients, healthcare providers (HCP), and the government. Rouse (2015) noted that personal health information (PHI) includes "medical and insurance records, demographics, lab test results, and any other detail gathered by health professionals to generate patient profiles for treatments." HCPs consist of individuals or organizations that are responsible for diagnosing, preventing, or treating a sickness or disability. HCPs are continually working to balance patient care with the protection of PHI privacy in health information systems (HIS). Efficiency and effectiveness in patient care have always been a key concern for the healthcare industry (Archer et al., 2011; Blumenthal and Tavenner, 2010). For this reason, many HCPs have focused on building and utilizing electronic medical record (EMR) systems (LeRouge and De Leo, 2010) that are geared toward retrieving patient information efficiently and effectively. (Appari and Johnson, 2010; Fernando and Dawson, 2009). However, while implementing an EMR system in the healthcare industry may seem to be a positive development, such developments might also be a harbinger of disaster concerning patient information privacy (Appari and Johnson, 2010; Datta et al., 2010; Goldschmidt, 2005). Because the rise of electronic information dispersal has made information privacy a key issue in healthcare, the U.S. government has adopted several laws to protect patients' PHI.

Today, there is a broad range of rules that regulate the association between patients and HCP. The Health Insurance Portability and Accountability Act (HIPAA, 1996) was introduced to address the copious amounts of patient privacy breaches that originated from HIS transactions (Moskop et al., 2005). The Health Information Technology for Economic and Clinical Health (HITECH, 2009) Act was introduced to

alleviate the side effects arising from the adoption of HIS and EMR. Also, in addition to these laws, Straton (2015) noted that the American Health Information Management Association (AHIMA), which represents over 100,000 health information professionals in the U.S. and around the world, has been extensively involved in taking measures to protect the privacy of PHI. AHIMA is focused on and dedicated to the growth and progression of health information professionals, encouraging high-quality research, best practices, and useful standards in health information worldwide (Stratton, 2015). Among the measures that AHIMA promotes are health information privacy and security, electronic health records, clinical documentation improvement, and information governance. AHIMA recommends proper HIS management to protect the privacy of the health records.

Although both the government and AHIMA seek to bolster and improve the efficiency and effectiveness of health information standards and health service transactions, privacy issues have paradoxically diminished the effect of these intentions (Angst and Agarwal, 2009; Chen and Xu, 2013; Goldschmidt, 2005; Wu et al., 2007). Problems still plague HCP, irrespective of these laws. Data breaches have become the norm in the industry. Based on Poneman Institute's "Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data," data breaches cost an estimated $6 billion. More than 90% of the healthcare providers studied had experienced a data breach, and 40% had experienced over five data violations within the last two years (Poneman, 2015).

The average cost of a data violation was over $2.1 million, which included over $1 million in data violations from business associates (Poneman, 2015). As defined by Poneman, "A Business Associate (BA) is a person or entity that performs services for a

covered entity that involves the use or disclosure of protected health information" (Poneman, 2015). Cochran et al. (2015) found that patients were deeply bothered by the privacy issues that arose from the use of electronic medical records (EMR) and healthcare information systems (HIS). Despite the laws and industry regulations aiming to protect personal health information, because of the statistics on healthcare data breaches, individuals are still anxious over their ability to control the privacy of their PHI.

The current research focuses on the impact of different control agencies in the perceived patient control over PHI in the presence of context-specific concerns. Control agencies are a product of personal and proxy control agencies. Personal control agency (PCA) mainly focuses on patients' capability to take control over the privacy of their PHI. Proxy control agencies (PRCA) are used when relying on HCP and government laws to protect patients' PHI. When there is a perception of some control over their own information, it is reported that individuals have fewer worries about their PHI privacy (Dinev and Hart, 2006, Xu et al., 2008). Conversely, Hoadley et al. (2010) stated that limited perceived control over personal information leads to a comparatively greater perception of privacy violations.

Control agency theory (Xu et al., 2012) served as the theoretical groundwork for this research. This represents the first time that control agency theory has been incorporated with healthcare information privacy. This was done to evaluate the impact of personal and proxy control agencies on perceived patient control over PHI in the presence of context-specific concerns. These context-specific concerns included collection, unauthorized access, errors, and secondary use. Collection refers to concerns

patients face when disseminating their PHI to an HCP and whether the data transfer is secure. Unauthorized access refers to patients' concerns over unauthorized parties (either organizational insiders or external parties) accessing PHI that has been entrusted to HCP. Errors refer to patients' concerns over the integrity or accuracy of their PHI as retained in HCP information systems; and secondary use refers to patients' concerns over unauthorized use and exploitation of their PHI. Since HCPs may trigger context-specific concerns for information privacy, CFIP acts as a moderator between HCP proxy control agency and perceived patient control over personal health information (CTL). Limitations in CTL lead to a comparatively greater perception of privacy violations, and this could be because of the limitations in control agencies and/or context-specific concerns, and/or the impact of control variables. This study will help to identify the role of personal and proxy control agencies and context-specific concerns in limiting or strengthening CTL. Identification of such limitations and issues will help patients, HCPs, and the government in strengthening their PHI protective measures. This research is a stepping stone for using control agency theory in the context of healthcare information privacy. Academicians can test this research model with different control agencies, such as the health insurance provider, the Patient Protection and Affordable Care Act (PPACA), and Medicare.

Chapter Two provides a summary of applicable literature to strengthen the main focus of the study. It also elaborates upon the research model and developed hypotheses. Chapter Three focuses on the research methodology, construct model, instrument design, and pilot study. Chapter Four comprises the data collection, analysis, and results, and Chapter Five concludes the study with contributions and limitations.

CHAPTER TWO

LITERATURE REVIEW

This chapter explores the literature applicable to the current research study and presents the study's research model and hypotheses.

General Privacy Definitions

General Privacy

If there is such a thing as general privacy as a human right, how did it begin (Schoeman, 1984)? Who is in charge of it (Milberg et al., 2000)? The prevailing view of privacy is derived from a standard of norms, and it may be unique to the law and culture of the specific country (Posner, 1978; Posner, 1981). When considering the roots of general privacy as a right in political theories, general privacy was not considered to be a protected right until the 20th century (Smith et al., 2011). Warren and Brandeis (1980) stated that general privacy is the right to be in isolation. Organizations and governments also equally desire the same right to privacy as individuals; organizations make an effort to maintain their competitive advantage by keeping certain information private, while governments desire to keep information safe from espionage (Giboney et al., 2014). Privacy policies have their trade-offs. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) provides privacy protections, but it also increases administrative costs and bureaucracy (Acquisti et al., 2004). There have been many

publications on privacy valuations in different arenas, and even highly secretive and privacy-conscious people have a tendency to share delicate data with others (Spiekermann et al., 2001). Based purely on the economic principle of revealed preferences, privacy does not have much importance in today's society, and thus it is questionable how to gauge the importance of privacy for individuals (Acquisti et al., 2004). After well-known repetitive attacks from privacy intruders, the U.S. federal government has imposed regulations and has offered advice and best practices for the protection of consumer information privacy (United States Census Bureau, 2010; U.S. Federal Trade Commission, 2010). Regardless, some authors have supported a self-regulatory framework, where individuals are responsible for making rational decisions about the privacy of their information (Acquisti et al., 2004). Individuals tend to conceal highly confidential or negative information about themselves and rationally share optimal information. The following list includes factors that may trigger greater or lesser privacy concerns among individuals: experiencing prior privacy violations (Smith et al., 1996); the individual's general knowledge about privacy-related practices (Cespedes and Smith, 1993; Malhotra et al., 2004); and the individual's knowledge about other privacy invading violations in the past (Giboney et al., 2014). If individuals have faced privacy violations or negative privacy experiences before (Smith et al., 2011, 1996), their privacy concerns are likely to be higher (Culnan, 1993; Smith et al., 1996; Stone and Stone, 1990; Wilson and Valacich, 2012). Individuals who have faced privacy violations will be more sensitive to such attacks and more likely to desire a defense against future attacks (Giboney et al., 2014). Also, an individual's knowledge about prior privacy violations

(from organizations collecting personal data) can lead to greater privacy concerns (Cespedes and Smith, 1993).

Privacy awareness is the degree of importance that appraisal individuals will attach to known privacy violations (Malhotra et al., 2004). Such an awareness might lead individuals to protect the privacy rights of others as well (Giboney et al., 2014). When an organization violates privacy rights and the public becomes aware of such violations (e.g., phone tapping conducted by the U.S. National Security Agency), the public is more ready to express their concerns about such activities (Giboney et al., 2014). The findings from prior research identify the current trend to view general privacy as a personal and public right.

Smith et al. (2011) conceptualized general privacy as having either a value or a cognate basis. Value-based privacy identifies privacy as a vital factor in shaping people's ethical standards, while cognate-based privacy views privacy as people's mental control over space and information (Smith et al., 2011). Additionally, economists have further investigated how consumers bargain privacy trade-offs and repercussions of their decisions (Acquisti et al., 2009). New and continued interest in privacy trade-offs can be seen in several papers from the mid-1990s (Varian, 1997; Noam, 1997; Loudan, 1997), while others explored privacy at the macroeconomic level (Taylor, 2004; Acquisiti and Varian, 2005; Calzolari and Pavan, 2006; Tang et al., 2008; Hann et al., 2007).

General privacy has been identified as a right in consumer behavior, leading to the paradoxical circumstance in which individuals willingly divulge their personal and confidential information for commercial gains (Smith et al., 2011). For this reason, privacy can be considered a commodity (Bennett, 1992). With this in mind, privacy is

an individual and social resource that can be attached to a commodity transaction based upon a cost-benefit value (Smith et al., 2011).

Privacy as a Commodity

It has been found that individuals voluntarily divulge their information based on a cost-benefit analysis (Campbell and Carlson 2002; Davies 1997; Garfinkel 2000). Smith et al. (2011) identified privacy as an "economical commodity which is subjected to cost-benefit analysis and trade-offs." Among many arguments by scholars with regard to defining general privacy, one popular idea is the market-based economic perspective of privacy, or privacy as a commodity. Such conclusions have been supported by real experimentations, where privacy and financial trade-offs are involved in hypothetical surveys (Acquisti, 2004). In Huberman et al.'s (2005) study, second price auction research was conducted to reveal the amount of money individuals would accept in exchange for making their weight or height public. Survey participants were comfortable giving out their personal data when financial benefits were presented (Wathieu and Friedman, 2007). Yet a significant difference was found in European Union citizens who were required to disclose their mobile data locations (Cvrcek et al., 2006). A field experiment was also conducted in Singapore to determine the types of privacy information and financial incentives people needed in order to disclose sensitive information (Hui et al., 2007). Again, a trade-off was found to exist between consumer evaluation of customization and privacy concerns (Chellappa and Sin, 2005). As reported in Tedeschi (2002), a Jupiter Research study found that a little over 80% of online shoppers were open to revealing their private information to a new website in order to

enter a $100 raffle draw. Sometimes individuals were also willing to exchange their private information for a minimal discount (Spiekermann et al., 2001).

Therefore, it is crucial to determine the fine line between the commodification of privacy and the treatment of privacy as a right. The paradoxical behavior that occurs around confidentiality and personal information is a consequence of disseminating such information without boundaries; as a result, markets should take privacy-guarding measures in order to control this dilemma (Laudon, 1997). With this in mind, privacy is an individual and social resource that can be attached to a commodity transaction based upon a cost-benefit value (Smith et al., 2011).

Cognate-Based Definitions

Westing (1968) first presented the concept of general privacy as a state and described it as having four different sub-dimensions: anonymity, solitude, reserve, and intimacy. Schoeman (1984) described privacy as a circumstance that restricts access to others. General privacy is a state of being in separation; compared to other types of seclusion, which are avoided and identified by individuals as a punishment in today's society, general privacy is a desired state (Weinstein, 1971). Lauter and Wolfe (1976) identified general privacy as a state that is made of self-ego, environmental, and interpersonal circumstances.

General Privacy as a Control

Westin's (1968) and Altman's (1975) conceptualization of general privacy leads to the conception of general privacy as a control. Margulis (1977a, 1977b) also suggested a control-focused general privacy definition, wherein privacy portrays the control of relations between two parties, which mainly aims to augment self-governance and/or to

lessen susceptibility. Since the late 1970s, privacy research has utilized the control-based classification of privacy, which has been further augmented in information systems and marketing research (Altman 1975; Culnan 1993; Kelvin 1973; Margulis 1977a; Smith et al. 1996; Westin 1968). Smith et al. (2011) stated that, although the initial definition equated privacy to control, the latest meanings refer instead to the capability to control.

Information systems researchers have indicated that control is one of the features that influence general privacy and that general privacy itself is not synonymous with control (Laufer and Wolfe, 1977; Margulis 2003a, 2003b). Laufer and Wolfe (1977) identified control as a mediator among the factors of general privacy systems, arguing that a situation cannot be categorized under general privacy just because an individual perceives, or has control over, the circumstances. Ironically, individuals may not recognize their control over privacy, because their surroundings and relationships may lead them to think otherwise (Laufer and Wolfe, 1977).

General vs. Context-Specific Concerns for Information Privacy

Based on previous research, the privacy concerns construct has consisted of two categories: general concerns over information privacy violations across all settings/background; and context-specific concerns for information privacy violations regarding a particular situation (Xu et al., 2012). Scholars such as Ackerman and Mainwaring from the field of computer science (2005) and Margulis from the field of sociology (2003a) have argued for a distinction between general and context-specific concerns for information privacy (Xu et al., 2012). For example, individuals' privacy standards may vary depending on specific and different situations and circumstances

(Ackerman and Mainwaring, 2005). The intensity of healthcare information privacy concerns may vary to a greater extent from that of social media information privacy concerns (Xu et al., 2012).

Xu et al. (2012) argues that the two types of privacy concerns are different from each other and have unique characteristics. They note that people's general concerns for information privacy can be a result of their upbringing, character, the societal emphasis on privacy, and the outlook toward sustaining privacy, which may not change across territories or contexts. Conversely, context-specific concerns might arise from people's valuation of privacy concerns within a specific context or from an external cause/mean, where the privacy concerns are assessed in relation to the need for releasing information (Sheehan, 2002). When these two privacy concerns are compared, context-specific privacy concerns take precedence over general privacy concerns (Li et al., 2011). Privacy should thus be investigated "at a specific level" (Malhotra et al., 2004). Mason's (1986) prediction that future generations will suffer from privacy issues because of the digital dissemination of information, has become inevitable in the current society.

Information Privacy

Although organizations may have privacy policies, the massive dispersal of mobile technologies and their limitless options for manipulating personal information have initiated consumer anxieties regarding privacy (Xu et al., 2012). With this in mind, Mason's (1986) predictions of future generations suffering from privacy issues because of the digital dissemination of information have already manifested (Belanger, 2011). Information privacy is a major concern among business executives, privacy activists,

academics, regulators, and individuals (Smith et al., 2011). Information privacy is defined as the desire of individuals to control or have some influence over data about themselves (Bélanger, 2011).

Although many disciplines have studied the concept of general privacy in the past 100 years, few have been successful in conceptualizing the term "information privacy" with a concrete definition. This could be because the paradoxical manner in which information privacy has operated, especially when it comes to online activities. Thus, scholars have found it difficult to conceptualize information privacy and to distinguish between information privacy and disclosure. Indeed, information privacy represents the fine line between information management and the public's stance on privacy. Information privacy violations often become a pressing issue when media exceeds the privacy limits of individuals, organizations, societies, and nations. Because of the fundamental alterations in technology since the inception of the information age, privacy has been one of the most predominant subjects in information systems research (Bélanger, 2011; Smith et al., 2011). Various studies, descriptions, and analyses have attempted to interpret the recent state of privacy research and to establish a foundation for future research (e.g., Appari and Johnson, 2010; Bélanger, 2011; Pavlou, 2011; Romanow et al., 2012; Smith et al., 2011). Although the exact nature of the balance remains enigmatic, the contradictory and challenging appeal of privacy often leads to arrangements in which individuals willingly divulge sensitive information (e.g., personalization) (Awad and Krishnan, 2006; Xu et al., 2011b). Smith et al. (2011) emphasized that, regardless of the substantial influence that privacy has on information systems, the privacy research stream has had a hard time coming up with an exact

definition for information privacy and an exact set of solutions for privacy violations. The continued technological advancements and the plethora of information processed in every form of online transaction (Conger et al., 2013) offer great value to all parties involved (Chen et al., 2012). The uses of private information also vary, as similar information can lead to different objectives and unique outcomes (Anderson and Agarwal, 2011; Conger et al., 2013). For example, a credit bureau can examine individual profiles for the purpose of providing loans based on each individual's credit history. However, if the same information is used inappropriately, the result can jeopardize individuals' identities and profiles. Likewise, within the healthcare environment, the proper use of individual information can immensely benefit patients. On the other hand, abuse of health records can lead to prejudice, humiliation, and even physical damage (Appari and Johnson, 2010; Brann and Mattson, 2004).

Health-Related Privacy

Personal health information (PHI) privacy is a primary area of interest for information systems research. Personal health information is considered to include documentation concerning personal medical records (Anderson, 1996). Although disclosure of such information and its facilitation through the use of electronic medical records (EMR) are seen as the most important aspects of privacy concerns in the health field, privacy issues are much more complex than can be expressed within these two areas alone (Anderson and Agarwal, 2011).

Health information systems generally operate separately and are often incompatible with other systems (Goldschmidt, 2005). Even though healthcare privacy information should be highly confidential, depending on the context it should also be

easily accessible by authorized parties. Since healthcare information systems (HIS) often operate independently, it may be difficult to disseminate required information among the involved parties. Unfortunately, such attempts to disseminate information can often lead to major concerns such as privacy breaches (Brann and Mattson, 2004; Petronio and Sargent, 2011). To alleviate delays and emphasize priorities, healthcare workers often engage in workarounds to make an HIS more efficient (Tucker, 2013). Even though efficiency and effectiveness are the goals in implementing HIS and EMR, these systems can paradoxically defeat their own purpose by creating privacy issues and workflow disruptions because of the adoption of strict privacy measures. For example, Choi et al. (2006) claimed that the Health Insurance Portability and Accountability (HIPAA) Act lowered the efficiency of healthcare system processes. The result of all these issues is that many healthcare professionals lack interest in implementing privacy safeguards (Bulgurcu et al., 2010).

When the U.S. passed HIPAA in 1996, it represented proof that health information privacy was finally accepted globally as an individual right (Appari and Johnson, 2010). HIPAA addresses the use and disclosure of individuals' health information by so-called "covered entities," and it presents standards for individuals' rights to understand and control how their health information is being used (HIPAA Privacy Rules). Additionally, the Health Information Technology for Economic and Clinical Health (HITECH, 2009) Act aims to enhance healthcare distribution and patient care by using a unique investment plan and automated healthcare information systems (in Summary of the HIPAA Privacy Rule). These plans and systems assist users and train

staff in operating electronic health records (EHRs), in order to benefit the general population (in Summary of the HIPAA Privacy Rule).

Also, AHIMA has endeavored to improve health information standards by adopting measures on subjects such as information privacy and security, electronic health records management, clinical documentation improvement, and information governance. Based on the AHIMA website, privacy and security issues are handled using HIPAA, the American Recovery and Reinvestment Act (ARRA) of 2009, and HITECH. AHIMA has published a policy and position statement on data copy and paste, a subject for which there is otherwise a lack of official guidance or practice standards. Additionally, AHIMA is focusing on maintaining the accuracy, timeliness, and scope of clinical documentations (AHIMA's Commitment to Healthcare—Information Governance, n.d.). As far as information governance, AHIMA's stance is "Like other critical organizational assets—people, capital, inventory, etc.—information is a strategic asset that requires a high level of oversight in order to be able to effectively use it for organizational decision-making, performance improvement, cost management, and risk mitigation." (AHIMA's Commitment to Healthcare—Information Governance, n.d.).

Although the intention of the public and private rule-making is to bolster and improve the efficiency and effectiveness of health information standards and health service transactions, patients are still forced to seek some sort of perceived control over information handed to HCPs because of ever-growing health record breaches. Patients tend to rely on either or both personal and proxy control agencies to protect their PHI privacy. In this study, control agency theory is used to illustrate the role of personal and proxy control agencies.

Control Agency Theory

Control perceptions can be divided into two aspects, based on the amount of direct and indirect control a person possesses. Direct control is achieved by having personal control, where individuals themselves act as the control agent (Bandura, 2001; Skinner, 1996). Personal control agency is preferred by most individuals, since they feel more confident over the level of control they possess (Yamaguchi, 2001). Individuals are more drawn to prospects that allow them to be the owner of their own actions (Bandura, 2001). Personal control agency is comparable with self-efficacy; thus, elaborating on self-efficacy in turn explains personal control agency. "The expectation of self-efficacy may influence feelings, thoughts, and actions. People with poor expectations tend to have low self-esteem and negative feelings regarding their abilities" (Gandoy-Crego et al., 2016). Protecting one's personal health information that has been handed to healthcare service providers is very challenging and difficult task. Regardless, patients feel that they have no choice but to protect their own personal health information because of the ever-growing number of healthcare privacy violations. Efficacious people set the bar high and pursue their goals with vigor (Gandoy-Crego et al., 2016). In this context, patients can take an active involvement in protecting their personal health information by taking actions such as keeping a watch on how their personal health information (PHI) has been collected, checking who has accessed their PHI, raising concerns about the accuracy and integrity of their PHI, and monitoring third party access to their PHI. Conversely, when patients have low self-efficacy, and/or are incapable of controlling the privacy of their health information because of the nature of the process, they can only gain control over privacy through other agents with authority (PCA).

Proxy control is when perceived control is gained through other agents with authority (Bandura, 2001; Yamaguchi, 2001). Individuals attempt to gain the desired outcomes through the help of powerful others in proxy control agencies (Bandura, 2001). Personal control is gauged using capacity, and proxy control agency is gauged using strategy. Capacity as used in this context can refer to either the degree of control one has over one's own actions or the perceived controllability (Azjen, 2002). Strategy is the amount of trust an individual has against other influences when completing a service transaction (Namasivayam, 2004).

Control action is defined by three sets of beliefs: control beliefs relating to an individual's control over the outcome of an event; strategy, which refers to utilizing other means with the authority or power to meet the person's desired ends; and capacity, which refers to the degree of access a person has to a particular cause (Namasivayam, 2004). Capacity and strategy determine an actor's control beliefs (Skinner, 1996). Namasivayam (2004) stated that the amount of control an individual has over environmental influences when completing a service transaction is known as strategy beliefs, and these beliefs influence an individual's feelings on taking control of a service exchange. At the same time, prior experience can play a significant role in an individual's capacity and strategy beliefs, meaning that an individual might be more interested in capacity than strategy beliefs in the inception of a new transaction (Namasivayam, 2004). Additionally, individuals depend on service providers to complete the intended transaction (Namasivayam, 2004).

Privacy Concerns as a Measurable Proxy for Privacy

Bandura (2001) stated that individuals rely on proxy control when they do not have the means or find it burdensome to take direct control. Although individuals use service providers as a proxy, they can quit the process at any time, such as when they are no longer satisfied with the transaction. In this study, the proxy control agencies under consideration are healthcare providers and the government. Both personal and proxy control agencies have a direct impact on the dependent variable, that of perceived patient control over PHI (CTL). Numerous studies have utilized Smith et al. (1996)'s concerns for information privacy (CFIP) scale with four data-related ranges of privacy concerns (collection, errors, secondary use, and unauthorized access to information) (Smith et al., 2011). These were later re-evaluated by Stewart and Segars (2002) and have proved to be the most trustworthy scales for gauging individuals' anxieties over "organizational privacy practices" (Smith et al., 2011). CFIP is comparable with the U.S. Federal Trade Commission's (FTC) fair information practices, which consist in *notifying* consumers when their personal information is gathered (equivalent to *collection* in CFIP), requesting *consent* when using the collected information (equivalent to *unauthorized secondary use* of individual information), *accessing* personal records to assure their correctness (equivalent to errors), and *securing* the records from unapproved access (equivalent to improper access). Similarly, Malhotra et al. (2004) utilized a multifaceted scale of Internet users' information privacy concerns. This represented the introduction of CFIP into the context of the Internet.

Perceived Patient Control over Personal Health Information (CTL)

Azjen (2002) mentioned that the perceived behavioral control arises through control beliefs. One's perception of taking action as a step toward accomplishing an end result is identified as perceived behavioral control (Namasivayam, 2004). In Azjen's (2002) hierarchical model, perceived behavioral control is described as a combination of perceived self-efficacy and controllability.

Perceived controllability is the amount of control an actor possesses in executing a task (Azjen, 2002). Hoadley et al. (2010) stated that a limited perceived control over personal information leads to a comparatively greater perception of privacy violations. Perceived control has been used as a substitute for actual control, because perception has been found to have a higher impact on an individual's actions than actual control (Skinner, 1996). An individual's sense of factors that might threaten the outcome of an action is normally identified as perceived control (Ajzen, 2002). Perceived control is a mental process, which may not lead to a direct action (Langer, 1975).

Smith et al. (2011) argued that, since there is no concrete explanation for privacy, nor any set of constructs to gauge it, intuition and opinions are used more than logical valuations in identifying privacy. Consequently, they opined that social science research depends on proxy constructs related to privacy (Smith et al., 2011). Although these proxies have been utilized under different names, information systems research have mainly focused on the privacy concerns construct (Smith et al., 2011).

The Impact of Control Agencies on Perceived Patient Control over Personal Health Information (CTL) in the Presence of Context-Specific Concerns

Figure 2.1 depicts the overall research model for the present study. This model shows the relationship between control agencies and CTL. It also shows the relationship between rival explanations and demographic controls and CTL. The context-specific concerns regarding information privacy moderate the relationship between the healthcare provider and CTL.

Perceived Patient Control over Personal Health Information in the Presence of Context-Specific Concerns

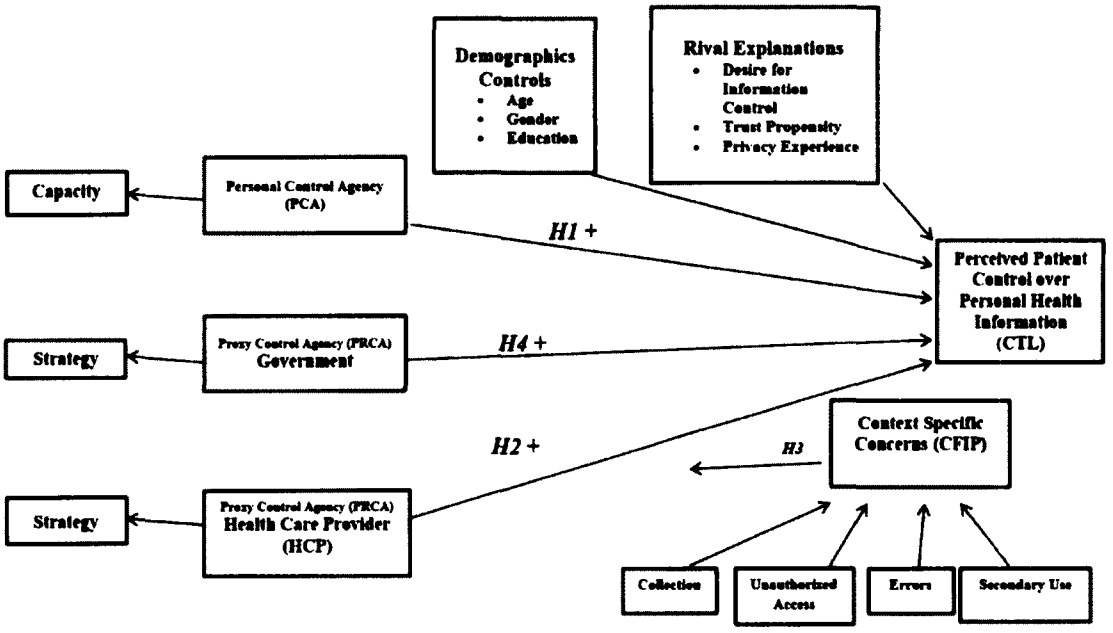


Figure 2.1 *Research Model*

Hypothesis Development

Personal Control Agency (PCA)

Personal control is when individuals act as their own control agent (Bandura, 2001; Skinner, 1996). Personal control agency is preferred by most individuals, because they feel more confident in the control they have over their personal information (Yamaguchi, 2001). When presented with the opportunity to have personal control of self-protection, individuals tend to opt for control over their environment (Weisz et al. 1984). Personal control gives confidence to individuals in managing the personal information that is collected by service providers. Examples of non-technological self-protection measures include refusal to reveal personal information, removal of personal information from mailing lists, complaints directly to companies using personal information, and complaints directly to third-party organizations (Xu et al., 2012).

Hypothesis 1 (H1): Personal control increases perceived patient control over personal health information (CTL)

Proxy Control Agency (PRCA)

Proxy control is when control over personal health information (PHI) is gained through other agents with authority (Bandura 2001, Yamaguchi 2001). Proxy control agency kicks in when individuals attempt to gain the outcomes with the help of powerful others (Bandura 2001). The current study focuses on two proxy control agencies: healthcare providers and the government.

Organizational Proxy Control Agency (OPRCA): Healthcare Provider (HCP)

In this case, OPRCA is gained through an HCP. HIPAA (1996) identifies a healthcare provider as a "provider of services, a provider of medical or health services,

and any other person or organization who furnishes bills, or is paid for healthcare in the normal course of business." HCPs collect, maintain, and disperse patients' EMR using one or more HIS, and these systems are highly vulnerable to unintentional or intentional breaches. In addition, because of the rapid growth of electronic health information dispersal and storage using electronic health records (EHR) and health information exchanges (HIEs), it is crucial to gauge the degree of trust that patients have in the provider's ability to protect their information (Hughes et al., 2014). According to the Health Information Privacy and Security 10-Step Plan (2013), healthcare providers can take these steps 90 days prior to adopting EHR:

(1) Confirm you are a 'covered entity,' which follows HIPAA responsibilities;

(2) Provide leadership—privacy and security officers;

(3) Document your process, findings, and actions—what security measures are present, and how they were created and monitored;

(4) Conduct security risk analysis—compare current security measures with the legal and realistic requirements;

(5) Develop action plans for addressing threats and vulnerabilities;

(6) Manage and mitigate risks;

(7) Prevent with workforce education and training risks;

(8) Communicate with patients;

(9) Update your business associate agreement; and

(10) Attest for the security risk analysis MU objective."

In addition to the aforementioned measures, healthcare providers may have other privacy measures in place, including frequent password change requests, different

password requirements for different systems and applications, and an automatic lock screen function after the system stays idle for a certain period, and data encryption. This leads to the Hypothesis 2.

Hypothesis 2 (H2): Healthcare provider proxy control increases perceived patient control over personal health information (CTL)

The Impact of Context-Specific Privacy Concerns (CFIP) on Healthcare Provider (HCP)

Research indicates that handling of information in organizations plays a key role in privacy concerns (Smith et al., 1996; Xu et al., 2011a). Such privacy concerns may arise because of an organization's inappropriate security (e.g., not encrypting confidential information), unapproved release (e.g., disseminating customer data to third parties), and/or unauthorized usage of a patient's private information (Pavlou, 2011). In this study, the patient's CFIP will arise from information handling by healthcare providers. Also, these concerns will affect the relationship between the healthcare provider and CTL. Therefore, it is hypothesized that context-specific concerns for information privacy (CFIP) moderate the relationship between healthcare provider proxy control agency and CTL.

Hypothesis 3 (H3): Context-specific concerns for information privacy (CFIP) moderate the relationship between HCP organization proxy control and perceived patient control over personal health information (CTL)

Organizational Proxy Control Agency (OPRCA): Government

The government is a regulatory body that imposes laws, regulations, policies, acts, and rules for the well-being of its governed population. This study focuses mainly

on the government's involvement in protecting electronic healthcare records and patients' private and confidential information. As privacy violations and record breaches continued to arise because of the adoption of HIS and EMR, the government introduced HIPAA in 1996 for the purpose of protecting patients and their rights. Subsequently, in 2009, the U.S. government introduced the HITECH Act to supplement HIPAA by training health professionals and patients to efficiently, effectively, and securely operate EMR and HIS. As a result, Hypothesis 4 is formed.

Hypothesis 4 (H4): Government proxy control increases perceived patient control over personal health information (CTL)

Control Variables (Rival Explanations)

The intensity of privacy concerns can vary because of the individual's emotional traits and demographic characteristics (Xu et al., 2012). This study focuses on three control variables—trust propensity, desire for information control, and privacy experience—and three demographic characteristics (Culnan, 1995, Malhotra et al., 2004)—age, gender, and education. Prior studies have found that individuals who are less educated, young, and males tend to have fewer privacy concerns (Culnan, 1995; Sheehan, 1999).

Trust propensity is the degree of faith an individual has for different people and situations (McKnight et al., 2002). Trust propensity can strengthen an individual's confidence in a specific context and thus reduce the individual's unique concerns over information privacy (Xu et al., 2012). The desire for information control is the individual's anticipated control over the amount and types of the organization's accumulation and manipulation of data (Phelps et al., 2000). Individuals with a higher

desire for information control have greater concerns over personal health information privacy violations than those who have a lower desire for information control (Xu et al., 2012). Based on prior good or bad privacy experiences, individuals may have greater or fewer privacy concerns (Smith et al., 1996).

Chapter Three focuses on this study's research methodology, construct model, and instrument design.

CHAPTER THREE

RESEARCH METHODOLOGY

This chapter illustrates the constructs, variables, and model that were used in the present research, followed by definition of the survey instrument, which was developed using valid and reliable constructs to test the model.

Constructs and Variables

An exploration of the literature on privacy reveals that control is commonly identified as ownership (Westin, 1968). It is an individual's right to exercise the choice to engage in electronic media exchange fully or partially (Caudill and Murphy, 2000), or the individual's ability to take control over the broadcasting of electronic information (Zweig and Webster, 2002). Attention is also given to the degree of control an individual has over all situations, such as when information is gathered and transferred (Schwartz, 1999). The norm "is that privacy assurance is not just a matter for the exercise of individual actions but also an important aspect of institutional structure" (Xu et al., 2012). Solve (2002) stated that privacy is a society's responsibility rather than an individual's right. The present study was conducted using the control agency theory (Xu et al., 2012) to gauge the perception of control that people have over their personal health information privacy. Control agency theory is comprised of both personal control agency, an individual's control over their own privacy (Bandura, 2001, Skinner, 1996),

and proxy control agency, where individuals depend on organizations with authority to protect their privacy (Namasivayam, 2004).

Personal Control Agency

Personal control agency focuses on an individual's self-efficacy in protecting his/her own privacy compared to depending on outsiders (Yamaguchi, 2001). In this situation, individuals exploit the choices they are given to take responsibility for their own behavior (Bandura, 2001). Personal control is gauged using capacity beliefs. Capacity beliefs refer to the degree of access a person has to a particular cause and are comparable with self-efficacy (Namasivayam, 2004).

Proxy Control Agency

In proxy control agency, individuals aim to gain control over their own privacy through powerful agents (Xu et al., 2012). Proxy control agency focuses on strengthening perceived control over privacy measures through others with authority (Bandura, 2001; Yamaguchi, 2001). Bandura stated that "people try by one means or another to get those who have access to resources or expertise or who wield influence and power to act at their behest to secure the outcomes they desire" (Bandura 2001). "Strategy" is used to gauge proxy control agency. Strategy refers to other means that are available for reaching the desired goals (Namasivayam, 2004). In this study, healthcare service providers (HCPs) and the government act as proxy control agencies. In addition to the influence of control agencies, perceived patient control over personal health information (CTL) is gauged using a scale adapted from Xu et al. (2012).

Perceived Patient Control over Personal Health Information (CTL)

The perceived control is the degree of control a person feels over the administration of his/her personal information (Xu et al., 2012). Control perception is influenced by two variables: personal control agency, having direct control over a situation or acting as one's own control agent (Bandura 2001, Skinner 1996); and proxy control agency, relying on other parties with authority to act as the control agent (Bandura 2001, Yamaguchi 2001).

Context-Specific Concerns for Information Privacy (CFIP)

CFIP is a second-order formative factor that is comprised of four first order items; those items are: collection—individuals' reaction and discomfort over the collection of their personal information); unauthorized access—individuals' uneasiness and doubt over the privacy of their personal information); errors—individuals' concern over the integrity of their personal information as stored in the information systems; and secondary use—individuals' distress over securing personal records from unapproved access (Smith et al., 2011).

Control Variables

The three control variables used in this research are: desire for information control, the degree of control an individual wishes to have over his/her own personal information as gathered and stored by organizations; trust propensity, the amount of trust an individual has over the interaction with others; and privacy experience, the individual's past experience in dealing with privacy situations (Xu et al., 2012). Table 3.1 shows the construct measurements used in the study.

Table 3.1

Construct Measurements

Construct	**Scale**
Control Agency	
Personal Control - Capacity	(Namasivayam, 2004)
Proxy Control - Strategy	(Namasivayam, 2004)
Context-Specific concerns for Information Privacy (CFIP)	(Xu, Heng., Teo, Hock-Hai., Tan, Bernard C. Y., and Ritu, 2012)
Perceived Patient Control over Personal Health Information (CTL)	(Xu, Heng., Teo, Hock-Hai., Tan, Bernard C. Y., and Ritu, 2012)
Desire for Information Control	(Xu, Heng., Teo, Hock-Hai., Tan, Bernard C. Y., and Ritu, 2012)
Trust Propensity	(Xu, Heng., Teo, Hock-Hai., Tan, Bernard C. Y., and Ritu, 2012)
Privacy Experience	(Xu, Heng., Teo, Hock-Hai., Tan, Bernard C. Y., and Ritu, 2012)

Model and Instrument Design

The current study will use a survey instrument to analyze the impact of different control agencies on the perceived patient control over personal health information (CTL) in the presence of context-specific concerns. This study extends the measures of personal control with capacity and proxy control with strategy, and for the first time it tests the extended model in the context of healthcare information privacy. Also, CFIP is used as a moderator between HCP proxy control agency and CTL to identify the impact of different context-specific concerns.

Preliminary Testing

A pretest and pilot test on the full questionnaire was performed (Boudreau et al., 2001; Straub, 1989). First, the pretest was conducted with the assistance of faculty members and doctoral students from a large university in the southeastern United States to analyze the content of the survey instrument. After analyzing the pretest recommendations, the survey instrument was altered as deemed necessary.

Next, an anonymous pilot study was conducted, with the assistance of students attending Computer Information Systems classes in the fall quarter of 2014, to test the readability and functionality of the survey instrument. The survey questionnaire was the product of items from each construct in the main model: moderator, control variables, and demographics. To verify the reliability of the responses, a few questions that held no relevance to the main study were added to the questionnaire (marker variables). These marker variables questions were supposed to be left alone without an answer, but if the respondents did not pay attention to the instructions and answered them anyway, those responses were discarded. To verify the reliability of the responses, a few questions that held no relevance to the main study were added to the questionnaire. These questions were supposed to be left alone without an answer, but if the respondents did not pay attention to the instructions and answered them anyway, those responses were discarded.

Primary Study

In an effort to save both time and money, data collection was conducted by means of an online survey distribution. The data collection for the primary study was done using a Qualtrics survey, which was distributed to the respondents by Mechanical Turk, Amazon's data collection platform. The data analysis was conducted using a second-

generation causal modeling statistical technique, the Smart Partial Least Squares (PLS) 3. The context-specific concerns for information privacy (CFIP) served as a second-order factor and were gauged using four formative variables: collection, unauthorized access, error, and secondary use. Gefen et al. (2000) suggested that the minimum sample size for the PLS technique should be "at least 10 times the number of items in the most complex construct." The most complex construct in this research is CFIP, which has 14 indicators; thus, the minimum sample required for testing the model is 140 respondents. As this research used 176 responses, it passed the threshold.

The College of Business at Louisiana Tech has been successful in its use of online panels, as such panels provide generalizable results while maintaining the complete anonymity of the respondents. Mechanical Turk confirms the demographic characteristics of the respondents while maintaining their anonymity even from the researchers. Table 3.2 presents a profile of the respondents.

Table 3.2

Profile of the Participants

	Frequency	Percentage
Gender		
Female	102	58%
Male	74	42%
Age		
18 to 30 yrs	56	31.8%
31 to 40 yrs	0	0%
41 to 50 yrs	33	18.8%
51 to 60 yrs	78	44.3%
Over 60 yrs	9	5.1%
Education		
High School Graduate	5	2.8%
Diploma	3	1.7%
Some Certification	4	2.3%

	Frequency	Percentage
Some College, No Degree	32	18.2%
Associate Degree	23	13.1%
Bachelor's Degree	90	51.1%
Master's Degree	16	9.1%
Doctorate or Ph.D. Professional Degree	2	1.1%
Other	1	0.6%
Current Health Insurance Status		
Yes	163	92.6%
No	13	7.4%%
Frequency of Visiting the Healthcare Provider Last Year		
Never	17	9.7%
1-2 Times	89	50.6%
3-6 Times	46	26.1%
7-10 Times	15	8.5%
More than 10 times	9	5.1%
Years of Employment		
Never	1	0.6%
1-2 yrs	10	5.7%%
3-6 yrs	28	15.9%
7-10 yrs	31	17.6%
More than 10 yrs	106	60.2%

CHAPTER FOUR

DATA ANALYSIS AND RESULTS

This chapter mainly focuses on the screening, cleaning, testing, and analysis of the data, the testing of the hypotheses, and the research findings.

Data Cleansing and Assumption Testing

Initial data screening was conducted to ensure the usability, reliability, and validity of the data for testing the proposed model (Hair et al., 2006). It was mandatory for respondents to answer each question in the survey before proceeding, to ensure there would be no concerns about missing data. The survey included attention checks, in order to weed out unengaged responses. Also, a variance check was conducted to delete any responses with low variances. An analysis for outliers was conducted only on latent variables. A few outliers were found under the categories of level of education, current health insurance status, frequency of visiting the healthcare provider, and years of employment, but these outliers were not abnormal and represented the sample. Because of the small sample size, these outliers were left in the dataset. The demographic variables of education, current health insurance status, and frequency of healthcare provider visits indicated some skewness and kurtosis issues. This was because 51.1% of respondents held bachelor's degrees, 92.6% had health insurance, and 50.6% visited

healthcare providers, compared to other categories with a lower percentage of respondents. In addition, there was some skewness in the CFIP collection and privacy experience indicators. Some of the respondents' desire for information control and trust propensity displayed kurtosis issues. Despite these issues, all variables had histograms with normal curves. The linearity of the variables was tested using composite values for the DV and each IV (Lowry and Gaskin, 2014). The results indicated that all IVs had a linear relationship with the DV. Though PLS does not require homogeneity of variance assumption (Lowry and Gaskin, 2014), a homogeneity of variance test was conducted for all variables, and it found that heterogeneity of the variance was not an issue with the dataset. The multicollinearity assumption was tested using the threshold of less than a 3.3 variance inflation factor (VIF) (Diamantopoulos and Siguaw, 2006; Petter et al., 2007). All composite variables were below the threshold and did not indicate any multicollinearity issue. However, when the CFIP variables were independently tested for the multicollinearity assumption, collection and unauthorized access (VIF 3.458) as well as secondary usage and unauthorized access (VIF 3.915) indicated values slightly above the threshold. But, since these were variables of a formative construct and the values were only slightly above the cut-off values of 3.3, it was determined that the multicollinearity was not an issue with the dataset.

Measurement Validation

First, the model was tested for the convergent and discriminant validity. As defined by Xu et al. (2012), "convergent validity is the degree to which different attempts to measure the same construct agree." The three measurements—reliability of items, composite reliability of constructs, and average variance extracted by constructs—were

used to gauge the convergent validity. Loadings for each item on the construct exceeded 0.65 and thus reflect adequate reliability (Hair et al., 2006). The findings were also above Nunnally's (1978) composite reliability threshold of 0.7. Also, the Cronbach's alphas were greater than 0.7, and average variance extracted for the constructs was above 0.5 (Table 4.1, Table 4.2, and Table 4.3). The discriminant validity was established based on the Fornell-Larckar criterion (Table 4.4), where the square root of the average variance extracted (AVE) on the diagonal was higher than the rest of the values (Hensler et al., 2015). The cross loadings, representing the correlation between the indicators and the construct to which they belong (Figure 4.1), were always higher compared to the relations with the other constructs (Hensler et al., 2015).

Table 4.1

Factor Analysis: Convergent and Discriminant Validity

Latent Factor	Item	CTL	DESIRE	GOVT	HCP	PCA	PE	TP
Perceived Control (CTL) : a = 0.95	CTL1	0.923	-0.268	0.353	0.283	0.235	-0.191	0.278
	CTL2	0.864	-0.278	0.252	0.243	0.205	-0.227	0.223
	CTL3	0.933	-0.254	0.267	0.264	0.239	-0.234	0.221
	CTL4	0.916	-0.249	0.292	0.273	0.182	-0.231	0.2
	CTL5	0.905	-0.315	0.265	0.228	0.235	-0.196	0.235
Desire for Information Control (DESIRE): a = 0.91	DESIRE1	-0.249	0.917	-0.119	0.051	0.137	0.082	-0.065
	DESIRE2	-0.285	0.938	-0.149	0.019	0.152	0.234	-0.149
	DESIRE3	-0.291	0.904	-0.108	0.024	0.036	0.145	-0.025
Strategy Government (GOVT): a = 0.96	GOVT 1	0.284	-0.109	0.957	0.446	0.094	-0.23	0.26
	GOVT 2	0.27	-0.101	0.953	0.461	0.032	-0.301	0.293
	GOVT 3	0.33	-0.125	0.965	0.484	0.033	-0.329	0.317
	GOVT 4	0.308	-0.181	0.931	0.447	0.075	-0.249	0.276
Strategy HCP (HCP) a = 0.96	HCP1	0.28	0.046	0.458	0.944	0.231	-0.136	0.318
	HCP2	0.249	0.031	0.466	0.948	0.208	-0.115	0.258
	HCP3	0.273	-0.002	0.464	0.932	0.219	-0.179	0.388
	HCP4	0.272	0.052	0.444	0.966	0.233	-0.114	0.336
Personal Control Agency HCP (PCA)	PCA1	0.203	0.116	0.076	0.247	0.937	0.116	0.113
	PCA2	0.23	0.11	0.048	0.223	0.971	0.108	0.109

Latent Factor	Item	CTL	DESIRE	GOVT	HCP	PCA	PE	TP
a = 0.98	PCA3	0.255	0.094	0.082	0.228	0.958	0.146	0.098
	PCA4	0.255	0.089	0.057	0.218	0.964	0.157	0.087
	PCA5	0.201	0.156	0.025	0.206	0.938	0.123	0.082
Privacy Experience (PE): a = 0.79	PE1	-0.173	0.095	-0.322	-0.203	0.074	0.873	-0.342
	PE2	-0.214	0.164	-0.291	-0.207	0.083	0.891	-0.314
	PE3	-0.204	0.161	-0.133	0.037	0.185	0.757	-0.17
Trust Propensity (TP) a = 0.82	TP1	0.236	-0.108	0.257	0.295	0.148	-0.26	0.901
	TP2	0.205	-0.029	0.187	0.338	0.085	-0.309	0.793
	TP3	0.215	-0.082	0.331	0.259	0.025	-0.271	0.876

Table 4.2

Cronbach's Alpha

Cronbach's Alpha	
CTL	0.947
DESIRE	0.909
GOVERNMENT	0.965
HCP	0.962
PCA	0.975
PE	0.793
TP	0.819

Table 4.3

Average Variance Extracted

Average Variance Extracted (AVE)	
CTL	0.826
DESIRE	0.846
GOVERNMENT	0.906
HCP	0.898
PCA	0.909
PE	0.710
TP	0.736

Table 4.4

Statistical Power Analysis

Statistical Power Analysis	
Number of Predictors	13
Observed	0.33
Probability Level	0.05
Sample Size	176
Observed Statistical Power	0.9999

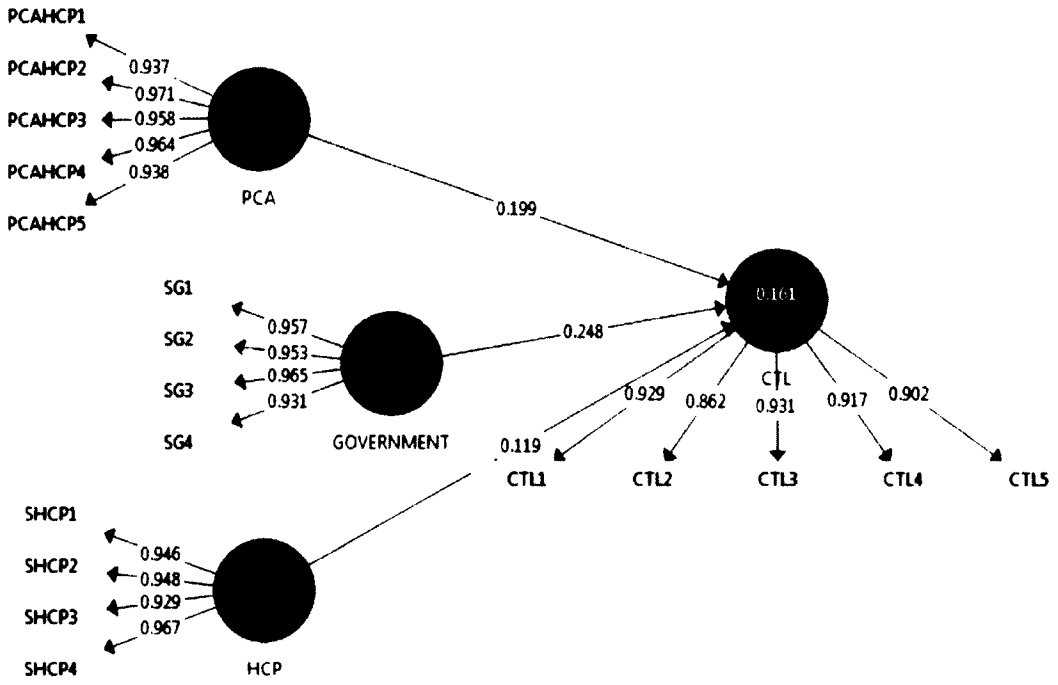


Figure 4.1 *The Main Effects Model*

As recommended by Lowry and Gaskin (2014), the molar model technique was used to analyze CFIP (Figure 4.2).

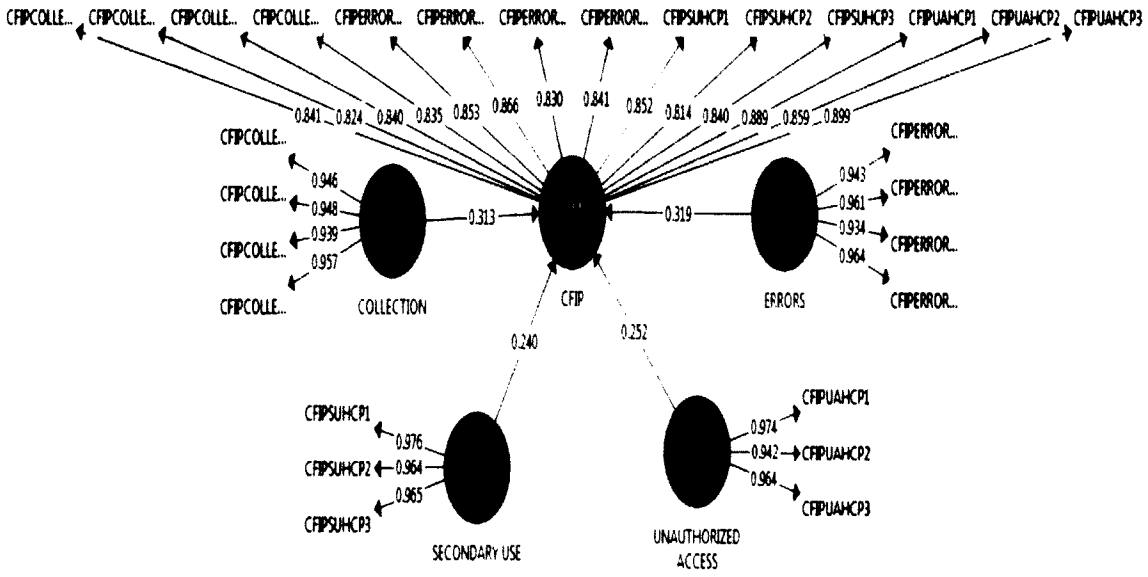


Figure 4.2 *CFIP: Second-Order Formative Factor*

Hypotheses Testing: Path Coefficients for Structural Model

Based on a posthoc statistical power calculation, the model demonstrated 99.99% power in detecting significant effects in this study (Table 4.5 and Figure 4.3) (Soper, 2006). Also, since PLS does not assess the model's goodness of fit, the predictive validity of the model was established by the overall R-value, the amount of variance explained by the perceived control over personal information (CTL), and paths with P values lower than 0.05 (Table 4.6) (Xu et al., 2012).

Table 4.5

Path Analysis

	Model 1 Interactions (Full) Model	**Model 2 Main Effects Model**
Proxy Control Agency		
Healthcare Provider		
Context-Specific Concerns for Information Privacy	-0.33**	
Perceived Control (CTL)		
Personal Control Agency (PCA)	0.3**	0.199**
Proxy Control Agency Government (GOVT)	0.08	0.25**
Proxy Control Agency Healthcare Provider (HCP)	0.00	0.12
Context-Specific Concerns for Information Privacy	-0.47**	
Moderating Effect	0.004	
R^2	**38.6**	**16.1**
Age	-0.029	
Gender	-0.058	
Education Level	-0.12	
Holding Health Insurance	0.10	
Healthcare Provider Visit	-0.071	
Work Experience	-0.054	
Desire for Information Control	-0.20**	
Trust Propensity	0.052	
Privacy Experience	-0.049	

*** p<0.05, ** p<0.01**

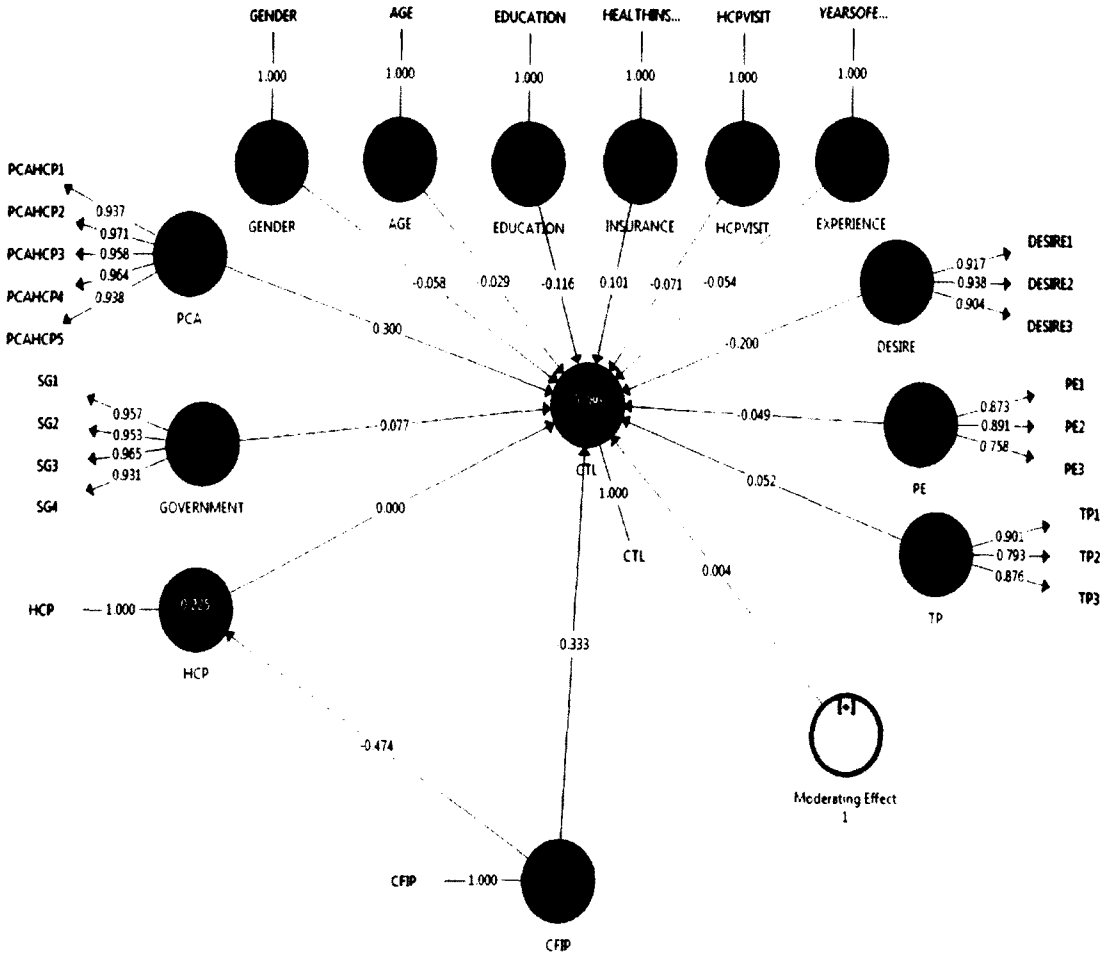


Figure 4.3 *Full Model*

Table 4.6

Hypotheses Testing

Hypothesis	Model	Outcome
H1: Personal control increases perceived patient control over personal health information (CTL)	*1*	Supported with a highly significant regression weight of 0.3
	2	Supported with a highly significant regression weight of 0.199
H2: Healthcare provider proxy control increases perceived patient control over personal health information (CTL)	1	Not supported
	2	Not supported
H3: Context-specific concerns for information privacy (CFIP) moderate the relationship between HCP organization proxy control and perceived patient control over personal health information (CTL)	1	Partially supported, since CFIP only affects HCP with a highly significant regression weight of -0.47. HCP does not impact CTL, but CFIP directly impacts CTL.
	2	Not a part of the latent variable model
H4: Government proxy control increases perceived patient control over personal health information (CTL)	1	Not supported
	2	Supported with a highly significant regression weight of 0.25

Based on the Table 4.6, personal control (PCA) increases perceived patient control over personal information (CTL) in both the main and latent models (Figures 4.3 and 4.1). Therefore, patients are more confident and comfortable in taking responsibility for their own healthcare privacy. The healthcare provider proxy control agency did not increase CTL. Context-specific concerns for information privacy (CFIP) partially moderated the relationship between HCP organization proxy control and CTL. Only the paths from CFIP to HCP and from CFIP to CTL were significant. CFIP negatively impacted or decreased HCP proxy control agency as well as CTL. The government proxy

control agency increased CTL in the main effects model but did not impact CTL in the full model. This could be because the control variable desire for information control had a significant -0.2 regression weight toward the CTL. According to the findings, when the desire for information control negatively impacted CTL, patients relied only on themselves to protect their personal health information and neglected or distrusted proxy control agencies.

CHAPTER FIVE

CONTRIBUTIONS AND LIMITATIONS

Contributions

Based on the prior literature, healthcare privacy violations have plagued the United States and have increased at an alarming rate since the inception of the information age (Poneman, 2015). Even with the many information privacy protection measures and remedies promulgated by practitioners and the government, healthcare information privacy violations are still a pressing and serious issue. The rest of this chapter focuses on the current study's contributions to practitioners and academia, as well as its limitations and recommendations. The findings of this study will assist patients, practitioners, and healthcare providers in strengthening the measures used to protect patients' personal health information. This study also offers help to the government in evaluating and strengthening HIPAA and HITECH.

Contributions to Patients and Practitioners

The findings of this study revealed that the three main factors affecting the perceived patient control over personal health information (CTL) were personal control over personal health information (PHI), desire for information control, and context-specific concerns for information privacy (CFIP). The first two factors, personal control and desire for information control, are all under the control of patients. As Bandura

(2001) noted, "The core features of agency enable people to play a part in their self-development, adaptation, and self-renewal with changing times." Over time, patients grow, change, and renew the degree of control they have over their personal health information. One factor that was parallel to personal control was the desire for information control. Patients, as owners of their own actions (Bandura, 2001), very much desire to control their own personal health information. As a result, the impact of government proxy control agency on the perceived control over personal health information was nullified once the desire for information control was introduced to the model.

Patients do have concerns about their health information privacy, even with all the information protection measures undertaken by healthcare providers and the government. Individuals with a greater desire for information control may have higher privacy concerns than individuals with a lower desire for information control (Phelps et al., 2000). The desire for information control affects context-specific concerns (Xu et al., 2012). Patients should be more vigilant and cautious, not only when providing their PHI to a healthcare provider, but also when seeking to understand how that information will be stored and used. Patients should have a higher desire for information control when they lack confidence in the healthcare information privacy protection measures provided by the government and by healthcare providers.

Healthcare providers and the government should pay closer attention to strengthening measures to thwart and alleviate the list of context-specific concerns for information privacy: collection (concerns patients face when disseminating their PHI to the HCP about whether the data transfer is secure); unauthorized access (patients'

concerns over unauthorized parties, either organizational insiders or external intruders, accessing PHI that they have entrusted to the HCP); errors (patients' concern over the integrity or accuracy of their PHI in the HCP information systems); and secondary use (patients' concerns over the unintended usage and exploitation of their information).

Contributions to Academia

This study reveals the impact of personal and proxy control agencies as well as context-specific concerns for information privacy (CFIP) on the perceived patient control over personal information (CTL). For the first time, the control agency theory is incorporated (Xu et al., 2012) to gain more insight on some of the factors that impact CTL. Also, the current research presents two constructs (Namasivayam, 2004) that can be used to gauge personal and proxy control agencies. An assessment was made of the impact of personal and proxy control agencies, context-specific concerns, control variables, and demographics on CTL. In the study reported herein, the main effect model indicated that the personal control agency and government proxy control agency increased CTL. However, as the desire for information control decreased the CTL, the impact that government had on CTL disappeared. Also, the moderator context-specific concerns for information privacy (CFIP) had a negative impact on the healthcare provider proxy control agency (HCP) as well as on CTL.

Limitations and Future Recommendations

The small sample size of 176 limits the overall generalizability of this study. This research only concentrates on the HCP proxy control agency and did not focus on the impact of other proxy control agencies, such as the health insurance provider proxy

control agency, on perceived patient control over personal information in the presence of context-specific concerns.

HCPs and the government should work together to strengthen their information privacy protection measures, especially when considering context-specific concerns for information privacy. Both parties can review and analyze the current measures to reveal the limitations of those measures. They can also start by strengthening these privacy measures one-by-one and can add new measures if warranted. Academicians can test the model presented herein with different control agencies as well as in different arenas, such as social media. For example, only two proxy control agencies were considered in this study. However, future researchers could include agencies such as health insurance providers, the Patient Protection and Affordable Care Act (PPACA), and Medicare. Also, future researchers can test this model in the context of social media, which also has prompted a plethora of user privacy issues since its inception.

APPENDIX A

SURVEY INSTRUMENT

Personal Control Agency (PCA) – Capacity (Namasivayam, 2004)

C1: I caused my healthcare provider (HCPs) to give me everything I needed for protecting my personal health information (PHI).
C2: I persuaded my HCPs to give me everything I needed for protecting my personal health information.
C3: I motivated my HCPs to give me everything I needed for protecting my PHI.
C4: I influenced my HCPs to give me everything I needed for protecting my PHI.
C5: I convinced my HCPs to give me everything I needed for protecting my PHI.

Organizational Proxy Control Agency (OPCA)

Strategy for Healthcare Provider (HCP) (Namasivayam, 2004)

HCP1: Everything required for protecting my personal health information (PHI) was available in the service exchange.
HCP2: My HCPs had everything required for protecting my PHI.
HCP3: My HCPs had implemented all essential measures to protect my PHI.
HCP4: The service encounter had everything essential for the protection of my PHI.

Strategy for the Government (SG) (Namasivayam, 2004)

This study concentrates on government laws HIPAA and HITECH.

Health Insurance Portability & Accountability Act (HIPAA)

The HIPAA Privacy Rule provides federal protections for individually identifiable health information held by covered entities and their business associates and gives patients an array of rights with respect to that information. At the same time, the Privacy Rule is balanced so that it permits the disclosure of health information needed for patient care and other important purposes.

Health Information Technology for Economic and Clinical Health (HITECH) Act

The Health Information Technology for Economic and Clinical Health (HITECH) Act promote the adoption and meaningful use of health information technology. Subtitle D of the HITECH Act addresses the privacy and security concerns associated with the electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules.

The Security Rule specifies a series of administrative, physical, and technical safeguards for covered entities and their business associates to use to assure the confidentiality, integrity, and availability of electronic protected health information.

G1: Everything required for protecting my personal health information (PHI) is available in government laws.

G2: The government laws have everything required for protecting my PHI.
G3: The government has implemented sufficient laws to protect my PHI.
G4: My PHI protection is assured by current government laws.

Context-Specific Concerns for Information Privacy (CFIP) (Xu et al. 2012)
Collection

COL1: It usually bothers me when healthcare providers (HCPs) ask me about my personal health information (PHI).
COL2: When HCPs ask me for my PHI, I sometimes think twice before providing it.
COL3: It bothers me to give my PHI to HCPs
COL4: I am concerned that HCPs are collecting too much PHI about me.

Unauthorized access

UA1: I am concerned that healthcare provider (HCPs) may not devote enough time and effort to prevent unauthorized access to my PHI.
UA2: I am concerned that the computer database that contains my PHI may not be well protected from unauthorized access.
UA3: I am concerned that HCPs may not take measures to prevent unauthorized access to my PHI.

Errors

E1: I am concerned that all the PHI in HCPs computer databases may not be double-checked for accuracy.
E2: I am concerned that HCPs may not take steps to make sure that my PHI in their database is accurate.
E3: I am concerned that HCPs may not establish the procedures necessary to correct errors in my PHI.
E4: I am concerned that HCPs may not devote time and effort to verify the accuracy of my PHI in their database.

Secondary use

SU1: I am concerned that HCPs may use my PHI for other purposes without notifying me or getting my authorization.
SU2: I am concerned that HCPs may sell my PHI in their database to other companies.
SU3: When I give my PHI to HCPs for the use of its service, I am concerned that the HCPs may use my information for other purposes.
SU4: I am concerned that HCPs may share my PHI with other parties without getting my authorization.

Perceived Patient Control over Personal Information (CTL)
Composite Reliability = .95, AVE = .79 (Xu et al. 2012)

PC1: How much control do you feel you have over your personal health information (PHI) that has been released?
PC2: How much control do you feel you have over the amount of your PHI collected?
PC3: Overall, how much in control do you feel you have over your PHI given to the others?
PC4: How much control do you feel you have over who can get access to your PHI?
PC5: How much control do you feel you have over how your PHI is being used by others?
PC6: If you are reading this question carefully, you will select strongly agree.

Trust Propensity
Composite Reliability = .83, AVE = .62 (Xu et al. 2012)
TP1: Most people are honest in their dealings with others.
TP2: Most people are knowledgeable in their field of work.
TP3: I usually trust people until they give me a reason not to trust them.

Desire for Information Control
Composite Reliability = .96, AVE = .88 (Xu et al. 2012)

DFIC1: Before I decide to provide my personal information to an organization, I wish the organization would inform me fully about the collection of my personal information.
DFIC2: Before I decide to provide my personal information to an organization, I wish I have more information about how my personal information would be used.
DFIC3: When providing my personal information to an organization, I wish I can indicate what aspects in my profile would be used for marketing and what aspects would not.

Privacy Experience
Composite Reliability = .88, AVE = .71 (Xu et al. 2012)

PE1: How often have you experienced incidents where your personal information was used by a company without your authorization?
PE2: How often have you been a victim of privacy invasion involving your personal information by a company?
PE3: How often have you heard or read during the past year about the misuse of personal information of consumers by a company?

Demographics

D1: Are you a male or a female?

- Male
- Female

D2: What is your age?

- 18 to 30 years old
- 31 to 40 years old
- 41 to 50 years old
- 51 to 60 years old
- Over 60 years old

D3: What is your highest level of education?

- High school graduate
- Diploma
- Some certifications
- Some college, no degree
- Associate degree
- Bachelor's degree
- Master's degree
- Doctorate or Ph.D. Professional degree

D4: Do you have health insurance?

- Yes
- No

D5: How many times have you gone to the healthcare provider since last year?

- 0
- 1-2
- 3-6
- 7-10
- More than 10

D7: How many years have you been employed?

- 0
- 1-2
- 3-6
- 7-10
- More than 10

APPENDIX B

HUMAN USE APPROVAL FORM

LOUISIANA TECH
UNIVERSITY
MEMORANDUM

OFFICE OF UNIVERSITY RESEARCH

TO: Dr. Selwyn Ellis and Ms. Prabhashi Nanayakkara

FROM: Dr. Stan Napper, Vice President Research & Development

SUBJECT: HUMAN USE COMMITTEE REVIEW

DATE: January 15, 2016

In order to facilitate your project, an EXPEDITED REVIEW has been done for your proposed study entitled:

"Perceived Patient Control over Personal Health Information in the Presence of Context-specific Concerns"

HUC 1387

The proposed study's revised procedures were found to provide reasonable and adequate safeguards against possible risks involving human subjects. The information to be collected may be personal in nature or implication. Therefore, diligent care needs to be taken to protect the privacy of the participants and to assure that the data are kept confidential. Informed consent is a critical part of the research process. The subjects must be informed that their participation is voluntary. It is important that consent materials be presented in a language understandable to every participant. If you have participants in your study whose first language is not English, be sure that informed consent materials are adequately explained or translated. Since your reviewed project appears to do no damage to the participants, the Human Use Committee grants approval of the involvement of human subjects as outlined.

Projects should be renewed annually. ***This approval was finalized on January 15, 2016 and this project will need to receive a continuation review by the IRB if the project, including data analysis, continues beyond January 15, 2017.*** Any discrepancies in procedure or changes that have been made including approved changes should be noted in the review application. Projects involving NIH funds require annual education training to be documented. For more information regarding this, contact the Office of University Research.

You are requested to maintain written records of your procedures, data collected, and subjects involved. These records will need to be available upon request during the conduct of the study and retained by the university for three years after the conclusion of the study. If changes occur in recruiting of subjects, informed consent process or in your research protocol, or if unanticipated problems should arise it is the Researchers responsibility to notify the Office of Research or IRB in writing. The project should be discontinued until modifications can be reviewed and approved.

If you have any questions, please contact Dr. Dr. Mary Livingston at 257-2292 or 257-5066.

REFERENCES

Ackerman MS, Mainwaring SD (2005) Privacy issues and human computer interaction. Garfinkel S, Cranor L, eds. *Security and Usability: Designing Secure Systems That People Can Use* (O'Reilly, Sebastopol, CA), 381–400.

Acquisti, Alessandro. 2004. Privacy in Electronic Commerce and the Economics of Immediate Gratification. Pp. 21–29 in *Proceedings of the Fifth ACM Conference on Electronic Commerce*, edited by Jack Breese, Joan Feigenbaum, and Margo Seltzer. New York: Association for Computing Machinery.

Acquisti, A., John, L., & Loewenstein, G. (2009, December). What is privacy worth? In *Workshop on Information Systems and Economics (WISE)*.

Acquisti, Alessandro, and Hal Varian. 2005. "Conditioning Prices on Purchase History." *Marketing* Science 24:1–15.

AHIMA's Commitment to Healthcare—Information Governance (n.d.). In *Information Governance*. Retrieved October 26, 2015, from http://www.ahima.org/topics/infogovernance/igbasics

Altman, I. 1975. *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding, Monterey*, CA: Brooks/Cole Publishing.

Anderson, Catherine L., and Ritu Agarwal. "The digitization of healthcare: boundary risks, emotion, and consumer willingness to disclose personal health information." *Information Systems Research* 22, no. 3 (2011): 469-490.

Angst, Corey M., and Ritu Agarwal. "Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion." *MIS Quarterly* 33, no. 2 (2009): 339-370.

Appari, Ajit, and M. Eric Johnson. "Information security and privacy in healthcare: current state of research." *International Journal of Internet and Enterprise Management* 6, no. 4 (2010): 279-314.

Archer, N., U. Fevrier-Thomas, Cynthia Lokker, K. Ann McKibbon, and S. E. Straus. "Personal health records: a scoping review." *Journal of the American Medical Informatics Association* 18, no. 4 (2011): 515-522.

Awad, Naveen Farag, and Mayuram S. Krishnan. "The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization." *MIS Quarterly* (2006): 13-28.

Ajzen, Icek. "Nature and operation of attitudes." *Annual Review of Psychology* 52, no. 1 (2001): 27-58.

Bandura, Albert. Social foundations of thought and action: *A Social Cognitive Theory.* Prentice-Hall, Inc, 1986.

Bandura, Albert. "Social cognitive theory: An agentic perspective." *Annual Review of Psychology* 52, no. 1 (2001): 1-26.

Bélanger, France, and Robert E. Crossler. "Privacy in the digital age: a review of information privacy research in information systems." *MIS quarterly* 35, no. 4 (2011): 1017-1042.

Bennett, Colin J. Regulating privacy: Data protection and public policy in Europe and the United States. Cornell University Press, 1992.

Blumenthal, David, and Marilyn Tavenner. "The "meaningful use" regulation for electronic health records." *New England Journal of Medicine* 363, no. 6 (2010): 501-504.

Boudreau, Marie-Claude, David Gefen, and Detmar W. Straub. "Validation in information systems research: a state-of-the-art assessment." *MIS Quarterly* (2001): 1-16.

Brann, Maria, and Marifran Mattson. "Toward a typology of confidentiality breaches in health care communication: An ethic of care analysis of provider practices and patient perceptions." *Health Communication* 16, no. 2 (2004): 231-251.

Bulgurcu, Burcu, Hasan Cavusoglu, and Izak Benbasat. "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness." *MIS Quarterly* 34, no. 3 (2010): 523-548.

Calzolari, Giacomo, and Alessandro Pavan. "On the optimality of privacy in sequential contracting." *Journal of Economic theory* 130, no. 1 (2006): 168-204.

Campbell, John Edward, and Matt Carlson. "Panopticon.com: Online surveillance and the commodification of privacy." *Journal of Broadcasting & Electronic Media* 46, no. 4 (2002): 586-606.

Caudill, Eve M., and Patrick E. Murphy. "Consumer online privacy: Legal and ethical issues." *Journal of Public Policy & Marketing* 19, no. 1 (2000): 7-19.

Cespedes, Frank V., and H. Jeff Smith. "Database marketing: New rules for policy and practice." *Sloan Management Review* 34, no. 4 (1993): 7.

Chellappa, Ramnath K., and Raymond G. Sin. "Personalization versus privacy: An empirical examination of the online consumer's dilemma." *Information Technology and Management* 6, no. 2-3 (2005): 181-202.

Chen, Hsinchun, Roger HL Chiang, and Veda C. Storey. "Business Intelligence and Analytics: From Big Data to Big Impact." *MIS Quarterly* 36, no. 4 (2012): 1165-1188.

Chen, Yunan, and Heng Xu. "Privacy management in dynamic groups: understanding information privacy in medical practices." In *Proceedings of the 2013 Conference on Computer Supported Cooperative Work*, pp. 541-552. ACM, 2013.

Choi, Young B., Kathleen E. Capitan, Joshua S. Krause, and Meredith M. Streeper. "Challenges associated with privacy in health care industry: implementation of HIPAA and the security rules." *Journal of Medical Systems* 30, no. 1 (2006): 57-64.

Chronology of Data Breaches. (2015, October). In Privacy Rights Clearing House. Retrieved October 25, 2015, from https://www.privacyrights.org/content/chronology-data-breaches

Clearinghouse, Privacy Rights. "A *Chronology* of *Data Breaches*." (2015).

Cochran, Gary L., Lina Lander, Marsha Morien, Daniel E. Lomelin, Jeri Brittin, Celeste Reker, and Donald G. Klepser. "Consumer Opinions of Health Information Exchange, e-Prescribing, and Personal Health Records." *Perspectives in Health Information Management* 12, no. Fall (2015).

Conger, Sue, Joanne H. Pratt, and Karen D. Loch. "Personal information privacy and emerging technologies." *Information Systems Journal* 23, no. 5 (2013): 401-417.

Culnan, Mary J. "How Did They Get My Name: An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use." *MIS Quarterly* (1993): 341-363.

Culnan, Mary J., and Priscilla M. Regan. "Privacy issues and the creation of campaign mailing lists." *The Information Society* 11, no. 2 (1995): 85-100.

Cvrcek, Dan, Marek Kumpost, Vashek Matyas, and George Danezis. "A study on the value of location privacy." In Proceedings of the 5th ACM Workshop on Privacy in Electronic Society, pp. 109-118. ACM, 2006.

Datta, Anupam, Nipun Dave, John C. Mitchell, Helen Nissenbaum, and Divya Sharma. "Privacy Challenges in Patient-centric Health Information Systems." In HealthSec. 2010.

Davies, Simon G. "Re-engineering the right to privacy: how privacy has been transformed from a right to a commodity." In *Technology and Privacy*, pp. 143-165. MIT Press, 1997.

Diamantopoulos, Adamantios, and Judy A. Siguaw. "Formative versus reflective indicators in organizational measure development: A comparison and empirical illustration." *British Journal of Management* 17, no. 4 (2006): 263-282.

Dinev, Tamara, and Paul Hart. "An extended privacy calculus model for e-commerce transactions." *Information Systems Research* 17, no. 1 (2006): 61-80.

Federal Trade Commission. "Privacy & Data Security Update." https://www.ftc.gov/reports/privacy-data-security-update-2015#how

Fernando, Juanita I., and Linda L. Dawson. "The health information system security threat lifecycle: An informatics theory." *International Journal of Medical Informatics* 78, no. 12 (2009): 815-826.

Gandoy-Crego, Manuel, Miguel Clemente, Cristina Gómez-Cantorna, Rubén González-Rodríguez, and Adela Reig-Botella. "Self-efficacy and Health: The SEH Scale." *American Journal of Health Behavior* 40, no. 3 (2016): 389-395.

Garfinkel, Simson. *Database Nation: The Death of Privacy in the 21st Century.*" O'Reilly Media, Inc.", 2000.

Gefen, David, Detmar Straub, and Marie-Claude Boudreau. "Structural equation modeling and regression: Guidelines for research practice." *Communications of the Association for Information Systems* 4, no. 1 (2000): 7.

Giboney, Justin, David Wilson, and Alexandra Drucikova. "An Individual's Views of the Right to Privacy of Other Individuals, Companies, and Governments: A Theoretical Perspective." (2014).

Goldschmidt, Peter G. "HIT and MIS: Implications of health information technology and medical information systems." *Communications of the ACM*48, no. 10 (2005): 68-74.

Hair, J., B. Black, B. Babin, R. Anderson, and R. Tatham. "Multivariate data analysis with readings Oklahoma." (2006).

Hann, Il-Horn, Kai-Lung Hui, Sang-Yong Tom Lee, and Ivan PL Png. "Overcoming online information privacy concerns: An information-processing theory approach." *Journal of Management Information Systems* 24, no. 2 (2007): 13-42.

HITECH Act. (n.d.). In Certification and EHR Incentives. Retrieved March 28, 2014, from http://www.healthit.gov/policy-researchers-implementers/hitech-act

Hoadley, Christopher M., Heng Xu, Joey J. Lee, and Mary Beth Rosson. "Privacy as information access and illusory control: The case of the Facebook News Feed privacy outcry." *Electronic Commerce Research and Applications* 9, no. 1 (2010): 50-60.

Huberman, Bernardo A., Eytan Adar, and Leslie R. Fine. "Valuating privacy."*IEEE Security & Privacy* 3, no. 5 (2005): 22-25.

HUGHES, PENELOPE P., and MELISSA M. GOLDSTEIN. "Privacy, Security, and Regulatory Considerations as Related to Behavioral Health Information Technology." *Behavioral Healthcare and Technology: Using Science-Based Innovations to Transform Practice* (2014): 224. – Reference

Hui, Kai-Lung, Hock Hai Teo, and Sang-Yong Tom Lee. "The value of privacy assurance: An exploratory field experiment." *MIS Quarterly* (2007): 19-33.

(n.d.). In Summary of the HIPAA Privacy Rule. Retrieved March 28, 2014, from http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/#endnotes

ITRC 2014. "2013 Data Breach Stats," *Identity Theft Resource Center*, pp. 1-17.

Kelvin, Peter. "A social-psychological examination of privacy." *British Journal of Social and Clinical Psychology* 12, no. 3 (1973): 248-261.

Langer, Ellen J. "The illusion of control." *Journal of personality and social Psychology* 32, no. 2 (1975): 311.

Lauter, Robert S., and Maxine Wolfe. "Privacy as a Concept and a Social Issue." (1976). Laudon, K. C. 1996. "Markets and Privacy," *Communications of the ACM* (39:9), pp. 92-104.

LeRouge, C. M., and De Leo, G. 2010. "Information Systems and Healthcare XXXV: Health Informatics Forums for Health Information Systems Scholars," *Communications of the Association for Information Systems* (27:7), pp 99-112.

Li, Han, Rathindra Sarathy, and Heng Xu. "The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors." *Decision Support Systems* 51, no. 3 (2011): 434-445.

Lowry, Paul Benjamin, and James Gaskin. "Partial least squares (PLS) structural equation modeling (SEM) for building and testing behavioral causal theory: When to choose it and how to use it." *IEEE Transactions on Professional Communication* 57, no. 2 (2014): 123-146.

Loudon, Janice K., Mary Ruhl, and Edelle Field. "Ability to reproduce head position after whiplash injury." *Spine* 22, no. 8 (1997): 865-868.

Malhotra, Naresh K., Sung S. Kim, and James Agarwal. "Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model." *Information Systems Research* 15, no. 4 (2004): 336-355.

Margulis, Stephen T. "Conceptions of privacy: Current status and next steps." *Journal of Social Issues* 33, no. 3 (1977): 5-21.

Margulis, Stephen T., ed. *Privacy as a Behavioral Phenomenon.* Society for the Psychological Study of Social Issues, 1977.

Margulis, Stephen T. "Privacy as a social issue and behavioral concept. *"Journal of Social Issues* 59, no. 2 (2003): 243-261.

Mason, Richard O. "Four ethical issues of the information age." *MIS Quarterly* (1986): 5-12.

McKnight, D. Harrison, Vivek Choudhury, and Charles Kacmar. "Developing and validating trust measures for e-commerce: An integrative typology." *Information Systems Research* 13, no. 3 (2002): 334-359.

Milberg, Sandra J., H. Jeff Smith, and Sandra J. Burke. "Information privacy: Corporate management and national regulation." *Organization Science* 11, no. 1 (2000): 35-57.

Moskop, John C., Catherine A. Marco, Gregory Luke Larkin, Joel M. Geiderman, and Arthur R. Derse. "From Hippocrates to HIPAA: privacy and confidentiality in emergency medicine—part I: conceptual, moral, and legal foundations." *Annals of Emergency Medicine* 45, no. 1 (2005): 53-59.

Namasivayam, Karthik. "Action control, proxy control, and consumers' evaluations of the service exchange." *Psychology & Marketing* 21, no. 6 (2004): 463-480.

Noam, Eli M. "Privacy and self-regulation: Markets for electronic privacy." *Privacy and Self-Regulation in the Information Age* (1997): 21-33.

Nunnally, Jum. "C. (1978). Psychometric Theory." (1978).

Pavlou, Paul A., Huigang Liang, and Yajiong Xue. "Understanding and mitigating uncertainty in online environments: a principal-agent perspective." *MIS Quarterly* 31, no. 1 (2006): 105-136.

Pavlou, Paul A. "State of the information privacy literature: where are we now and where should we go?" *MIS Quarterly* 35, no. 4 (2011): 977-988.

Petronio, Sandra, and Jack Sargent. "Disclosure predicaments arising during the course of patient care: nurses' privacy management." *Health Communication* 26, no. 3 (2011): 255-266.

Petter, Stacie, Detmar Straub, and Arun Rai. "Specifying formative constructs in information systems research." *MIS Quarterly* (2007): 623-656.

Phelps, Joseph, Glen Nowak, and Elizabeth Ferrell. "Privacy concerns and consumer willingness to provide personal information." *Journal of Public Policy & Marketing* 19, no. 1 (2000): 27-41.

Ponemon Institute. 2007. "Database Security 2007: Threats and Priorities within IT Database Infrastructure," Traverse City, MI (available at http://www.appsecinc.com/techdocs/whitepapers/ 2007-Ponemon-Database-Security-Study-Sponsoredby- Application-Security-Inc.pdf)

Ponemon Institute. 2015. "2015 Cost of Cyber Crime Study: Global," pp. 1-29.

Ponemon Institute. 2015. "2015 Cost of Cyber Crime Study: The United States," pp. 1-29.

Ponemon Institute. 2015. "Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data," pp. 1-41.

Posner, Richard A. "The economics of privacy." *The American Economic Review* 71, no. 2 (1981): 405-409.

Posner, Richard A. "Economic theory of privacy." *Regulation* 2 (1978): 19.

Privacy, Commercial Data. "Innovation in the Internet Economy: A Dynamic Policy Framework." *Department of Commerce* 12 (2010): 16.

Rachels, James. "Why privacy is important." *Philosophy & Public Affairs* (1975): 323-333.

Romanow, Darryl, Sunyoung Cho, and Detmar Straub. "Editor's comments: riding the wave: past trends and future directions for health IT research." *MIS Quarterly* 36, no. 3 (2012): III-A18.

Rouse, M. (2015, June). In protected health information (PHI) or personal health information. Retrieved June 29, 2016, from http://searchhealthit.techtarget.com/definition/personal-health-information

Schoeman, Ferdinand David. *Philosophical Dimensions of Privacy: An Anthology*. Cambridge University Press, 1984.

Schwartz, Shalom H. "A theory of cultural values and some implications for work." *Applied Psychology* 48, no. 1 (1999): 23-47.

Sheehan, Kim Bartel. "Toward a typology of Internet users and online privacy concerns." *The Information Society* 18, no. 1 (2002): 21-32.

Skinner, Ellen A. "A guide to constructs of control." *Journal of Personality and Social Psychology* 71, no. 3 (1996): 549.

Smith, H. Jeff, Sandra J. Milberg, and Sandra J. Burke. "Information privacy: measuring individuals' concerns about organizational practices." *MIS quarterly* (1996): 167-196.

Smith, H. Jeff, Tamara Dinev, and Heng Xu. "Information privacy research: an interdisciplinary review." *MIS Quarterly* 35, no. 4 (2011): 989-1016.

Soper, D. "Post-hoc statistical power calculator for multiple regression." *Statistical Calculator* (2014).

Spiekermann, Sarah, Jens Grossklags, and Bettina Berendt. "E-privacy in 2nd generation E-commerce: privacy preferences versus actual behavior." In *Proceedings of the 3rd ACM Conference on Electronic Commerce*, pp. 38-47. ACM, 2001.

Staff, F. T. C. "Protecting Consumer Privacy in an Era of Rapid Change–A Proposed Framework for Businesses and Policymakers." *Journal of Privacy and Confidentiality* 3, no. 1 (2010): 5.

Stewart, Kathy A., and Albert H. Segars. "An empirical examination of the concern for information privacy instrument." *Information Systems Research*13, no. 1 (2002): 36-49.

Stone, Eugene F., and Dianna L. Stone. "Privacy in organizations: Theoretical issues, research findings, and protection mechanisms." *Research in Personnel and Human Resources Management* 8, no. 3 (1990): 349-411.

Stratton, B. (2015, July 28). AHIMA Survey: Growing Support for Making Information Governance a Priority in Healthcare Organizations. In IG News. Retrieved October 26, 2015, from file:///C:/Users/nanayakkaras/Downloads/N150728%20AHIMA%20Cohasset%20survey%20on%20IG%20white%20paper_FINAL.pdf

Straub, Detmar W. "Validating instruments in MIS research." *MIS Quarterly* (1989): 147-169.

Tang, Zhulei, Yu Hu, and Michael D. Smith. "Gaining trust through online privacy protection: Self-regulation, mandatory standards, or caveat emptor." *Journal of Management Information Systems* 24, no. 4 (2008): 153-173.

Taylor, Curtis R. "Consumer privacy and the market for customer information." *RAND Journal of Economics* (2004): 631-650.

Tedeschi, Bob. "Everybody talks about online privacy, but few do anything about it." *New York Times* 3 (2002): 6.

Tucker, Anita L., and Morgan Hall. *Work Design Drivers of Organizational Learning about Operational Failures: A Laboratory Experiment on Medication Administration.* No. 13-044. Working paper, 2013.

United States Census Bureau. http://www.census.gov/privacy/

Varian, Hal R. "Versioning information goods." (1997).

Wathieu, Luc, and Allan A. Friedman. "An empirical approach to understanding privacy valuation." *HBS Marketing Research Paper* 07-075 (2007).

Warren, Samuel D., and Louis D. Brandeis. "The right to privacy." *Harvard Law Review* (1890): 193-220.

Weinstein, Wendy L. "The private and the free: A conceptual inquiry." *Privacy: Nomos XIII* (1971): 624-692.

Weisz, John R., Fred M. Rothbaum, and Thomas C. Blackburn. "Standing out and standing in: The psychology of control in America and Japan." *American Psychologist* 39, no. 9 (1984): 955.

Westin, Alan F. "Privacy and freedom." *Washington and Lee Law Review* 25, no. 1 (1968): 166.

Wilson, Dave, and Joseph S. Valacich. "Unpacking the privacy paradox: Irrational decision-making within the privacy calculus." (2012).

Wu, Jen-Her, Shu-Ching Wang, and Li-Min Lin. "Mobile computing acceptance factors in the healthcare industry: A structural equation model." *International Journal of Medical Informatics* 76, no. 1 (2007): 66-77.

Xu, Heng, Tamara Dinev, H. Jeff Smith, and Paul Hart. "Examining the formation of individual's privacy concerns: Toward an integrative view." *ICIS 2008 Proceedings* (2008): 6.

Xu, Heng, Tamara Dinev, Jeff Smith, and Paul Hart. "Information privacy concerns: Linking individual perceptions with institutional privacy assurances." *Journal of the Association for Information Systems* 12, no. 12 (2011): 798.

Xu, Heng, Xin Robert Luo, John M. Carroll, and Mary Beth Rosson. "The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing." *Decision Support Systems* 51, no. 1 (2011): 42-52.

Xu, Heng, Hock-Hai Teo, Bernard CY Tan, and Ritu Agarwal. "Research note-effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: A study of location-based services." *Information Systems Research* 23, no. 4 (2012): 1342-1363.

Yamaguchi, Susumu. "Culture and control orientations." *The Handbook of Culture and Psychology* (2001): 223-243.

Zweig, David, and Jane Webster. "Where is the line between benign and invasive? An examination of psychological barriers to the acceptance of awareness monitoring systems." *Journal of Organizational Behavior* 23, no. 5 (2002): 605-633.