PRIVACY IN ONLINE COMMUNITIES: HOW CONTROL AND ASSURANCES INFLUENCE INTENTION TO DISCLOSE PERSONAL INFORMATION

Oscar E. Lopez Arizaga
University of Massachusetts Amherst

Follow this and additional works at: https://scholarworks.umass.edu/dissertations_2

Part of the Business Administration, Management, and Operations Commons, Management Information Systems Commons, and the Technology and Innovation Commons

Recommended Citation

This Open Access Dissertation is brought to you for free and open access by the Dissertations and Theses at ScholarWorks@UMass Amherst. It has been accepted for inclusion in Doctoral Dissertations by an authorized administrator of ScholarWorks@UMass Amherst. For more information, please contact scholarworks@library.umass.edu.
Privacy in Online Communities: How Control and Assurances Influence the Intention to Disclose Personal Information

A Dissertation Presented

By

Oscar E. Lopez-Arizaga

Submitted to the Graduate School of the University of Massachusetts Amherst in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

May 2022

Management
Privacy in Online Communities: How Control and Assurances Influence the Intention to Disclose Personal Information

A Dissertation Presented

By

Oscar E. Lopez-Arizaga

Approved as to style and content by:

__________________________________________________
Traci J. Hess, Chair

__________________________________________________
Yi (Zoe) Zou, Member

__________________________________________________
Linda M. Isbell, Member

__________________________________________________
George Milne, Phd. Program Director
Isenberg School of Management
ACKNOWLEDGMENTS

I would like to express my most sincere and profound gratitude to my advisor, Dr. Traci J. Hess for the long nights of dedication during the last few years. Her guidance, wisdom, patience, and above all her example of impeccable work ethic have made me a better professional and a better person. The memory of her kindness and generosity will live with me always.

To the members of my dissertation committee, Dr. Linda Isbell and Dr. Yi Zou for their support and guidance.

To my fellow PhD students in the Information Systems program at UMass Amherst, Ari Wigdor and Long Nguyen for always being available to answer questions, offer advice and making these years of study enjoyable.

My most special recognition and gratitude to my wife and children, Veronica, Martina and Mateo for having surrendered so many hours of their husband and father’s time and for their love and patience.
ABSTRACT

PRIVACY IN ONLINE COMMUNITIES: HOW CONTROL AND ASSURANCES INFLUENCE THE INTENTION TO DISCLOSE PERSONAL INFORMATION

MAY 2022

OSCAR E. LOPEZ-ARIZAGA, B.A., UNIVERSIDAD SAN FRANCISCO DE QUITO

M.Ed., GRAND VALLEY STATE UNIVERSITY

M.B.A., FLORIDA ATLANTIC UNIVERSITY

Ph.D., UNIVERSITY OF MASSACHUSETTS AMHERST

Directed by: Professor Traci J. Hess

Information Systems (IS) research has a long history of addressing privacy concerns with the use of IS. In the internet era, the proliferation of social network sites represents a highly relevant and fertile new context for the study of privacy. Specifically, special interest network sites such as online health communities provide a rich, context-specific scenario for the study of privacy, which promises to enhance our knowledge of this complex phenomena. Online communities are only successful to the extent that individuals join and participate in the communities, and privacy concerns are a barrier to this success. In this dissertation, the privacy calculus and the agentic perspective of social cognitive theory provide the theoretical foundation for studying privacy in online communities. This theoretical foundation provides insight on how control, privacy assurances, and information sensitivity can influence relevant outcomes such as risk, trust, and an individual’s intention to disclose personal information online.
The first study of this dissertation presents a comprehensive literature review of online privacy in IS. A number of research opportunities are found in the literature including limited empirical work on the roles of control and information sensitivity in the privacy phenomena. Additionally, privacy assurances are identified as an area needing further exploration from an interface design perspective. Finally, the causal nature of two important privacy-related constructs: risk and trust, are identified as experiencing notable tension in the extant literature. These gaps, identified by the literature review, provide research opportunities which the subsequent chapters in this dissertation address.

The first empirical study consists of an experiment manipulating control, privacy assurances and information sensitivity, and the effects on privacy concerns, risk, trust, and intention to disclose information online. The privacy calculus is introduced as the theoretical background for this study, and the research model confirms the neglected importance of control in the IS privacy literature. This chapter’s findings also shed light on the nature of the formation of trust and risk when individuals transact online. The privacy calculus theoretical model is fully adopted and expanded via this study which provides practitioner-level insights for the visual aspects of the web artifact that have a bearing on the user experience and intentions to disclose information.

The second empirical study of this dissertation digs deeper into the role of control in the privacy phenomena and incorporates a richer contextualization of control based on the agentic perspective of social cognitive theory. This factorial design experiment utilizes a survey and a fictitious, online health community website to investigate the effect of three different types of control (personal, proxy and collective) on risk, trust and intention to disclose. The different types of control identified in the theory are found to
have a complementary effect on different aspects of the phenomena. A model comparison via structural equation modeling is provided to expand the understanding of the directional relationship between risk and trust.

The findings of the three studies forming this dissertation provide a series of insights and research opportunities which constitute important contributions to the privacy literature in IS. The two experimental studies complement the existing research on privacy, illuminating the importance of control in studies of privacy and how privacy assurances can enhance trust in an online community. A closer analysis of important privacy constructs sheds light on the nature and boundary settings of online privacy and online health community privacy issues. Finally, both empirical studies of this dissertation work in conjunction to explore whether privacy concerns, a popular construct in the literature, can be seen as context-specific or as context-independent. Taken together, this dissertation expands our understanding of privacy concerns in online communities and discovers new applications of important constructs previously not addressed by the literature.
TABLE OF CONTENTS

ACKNOWLEDGMENTS .................................................................................................................. iv

ABSTRACT .................................................................................................................................. v

CHAPTER

1. INTRODUCTION ................................................................................................................... 1

1.1 Online Privacy and Privacy Concerns in IS Research ..................................................... 1

1.2 Organization of the Dissertation Manuscript ................................................................ 5

2. PRIVACY IN ONLINE HEALTH COMMUNITIES .............................................................. 8

2.1 Introduction ....................................................................................................................... 8

2.2 Literature Review: Privacy and online health communities ....................................... 11

2.2.1 Privacy ......................................................................................................................... 11

2.2.2 Theory in Privacy Research ....................................................................................... 15

2.2.3 Online Health Communities .................................................................................... 16

2.3 Methodology ................................................................................................................... 18

2.3.1 Journal Selection ........................................................................................................ 18

2.3.2 Article Selection ......................................................................................................... 20

2.3 Discussion of Empirical Studies ..................................................................................... 21

2.4.1 Focal Privacy-Related Constructs ............................................................................ 23

2.4.2 Privacy Concerns ......................................................................................................... 25

2.4.3 Perceived Privacy Risks ............................................................................................. 29

2.4.4 Other Privacy Focal Constructs ............................................................................... 31

2.4.5 Antecedents to Privacy-Related Constructs .............................................................. 33

2.4.5.1 Internal Antecedents of Privacy ......................................................................... 35

2.4.5.2 External Antecedents to Privacy ........................................................................ 40

2.4.6 Outcomes to Privacy-Related Constructs in the Literature .................................... 42
3.6.1 Theoretical Contributions .................................................................................... 85
3.6.2 Practical Implications ........................................................................................... 89
3.7 Conclusion and Limitations ........................................................................................ 91
Appendix: Website descriptions and instructions to experiment participants. ............... 93

4. MAXIMIZING PRIVACY CONTROL: THE ROLE OF PERSONAL, PROXY AND COLLECTIVE CONTROL IN ONLINE COMMUNITY INFORMATION DISCLOSURE .................................................................................................................. 95

4.1 Introduction ................................................................................................................. 95

4.2 Theoretical Background .............................................................................................. 98

4.2.1 Privacy and Control ............................................................................................. 98
4.2.2 Privacy & Privacy Concerns ................................................................................ 98
4.2.3 Risk and Trust in Privacy Studies ........................................................................ 99
4.2.4 Motivation to Disclose - Personal Internet Interest ........................................... 100
4.2.5 Theory and the Privacy Calculus ....................................................................... 100
4.2.6 Privacy Assurance .............................................................................................. 101
4.2.7 The Agentic Perspective of Privacy Control ..................................................... 102

4.3 Research Model and Hypotheses .............................................................................. 104

4.4 Study Design ............................................................................................................. 114

4.4.1 Participants ......................................................................................................... 114
4.4.2 Experimental Process ......................................................................................... 114
4.4.3 Construct Operationalization ............................................................................. 115

4.5 Results ....................................................................................................................... 119

4.5.1 Manipulation checks .......................................................................................... 120
4.5.2 Measurement Validity and Reliability ................................................................ 121

4.6 Analysis and Results ................................................................................................. 122

4.6.1 Structural Regression Model .............................................................................. 124
4.7 Discussion and Contributions ................................................................. 127
4.8 Conclusion and Limitations ................................................................. 132

5. IMPLICATIONS, FUTURE RESEARCH AND CONCLUSION .................... 133

5.1 Summary of Chapters ............................................................................. 133
5.2 Conceptual and Theoretical Implications ............................................... 133
5.3 Practical Implications ............................................................................. 136
5.4 Future Research ..................................................................................... 137

BIBLIOGRAPHY ......................................................................................... 139
### LIST OF TABLES

<table>
<thead>
<tr>
<th>Table</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1 - List of consulted journals &amp; search stage</td>
<td>19</td>
</tr>
<tr>
<td>2.2 - Privacy-related constructs in the literature</td>
<td>22</td>
</tr>
<tr>
<td>2.3 - Classification of antecedents to privacy-related constructs in the literature</td>
<td>37</td>
</tr>
<tr>
<td>2.4 - Outcomes in the privacy literature</td>
<td>42</td>
</tr>
<tr>
<td>3.1 - Survey Items</td>
<td>76</td>
</tr>
<tr>
<td>3.2 - Mean scores for all variables by treatment</td>
<td>77</td>
</tr>
<tr>
<td>3.3 - Manipulation check scores</td>
<td>78</td>
</tr>
<tr>
<td>3.4 - Study items’ loadings and cross-loadings from EFA</td>
<td>79</td>
</tr>
<tr>
<td>3.5 - Reliability, Correlations and AVE</td>
<td>80</td>
</tr>
<tr>
<td>3.6 - MANCOVA Results</td>
<td>82</td>
</tr>
<tr>
<td>3.7 - Interaction effects of Control and Assurance on Trust</td>
<td>83</td>
</tr>
<tr>
<td>3.8 - Structural Model Fit Statistics</td>
<td>84</td>
</tr>
<tr>
<td>3.9 - Hypotheses results</td>
<td>85</td>
</tr>
<tr>
<td>4.1 - Scales used in Pre and Post Surveys</td>
<td>118</td>
</tr>
<tr>
<td>4.2 - Descriptive Statistics - Means by Treatment</td>
<td>120</td>
</tr>
<tr>
<td>4.3 - Manipulation Check Analysis</td>
<td>120</td>
</tr>
<tr>
<td>4.4 - Reliability, Correlations, and Average Variance Extracted</td>
<td>121</td>
</tr>
<tr>
<td>4.5 - Factor Loadings from Exploratory Factor Analysis</td>
<td>122</td>
</tr>
</tbody>
</table>
4.6 - MANCOVA results ................................................................................................ 123

4.7 - Structural Regression Model Fit Statistics ...................................................... 124

4.8 - Hypotheses Results ......................................................................................... 125

4.9 - Alternative Models and Fit Statistics ............................................................... 126
<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 2.1</td>
<td>Integrated Nomological Map of Privacy Studies</td>
<td>48</td>
</tr>
<tr>
<td>Figure 3.1</td>
<td>The Privacy Calculus Model</td>
<td>60</td>
</tr>
<tr>
<td>Figure 3.2</td>
<td>The Research Model</td>
<td>64</td>
</tr>
<tr>
<td>Figure 3.3</td>
<td>Home page for the 2 companies (High Privacy Assurances condition)</td>
<td>74</td>
</tr>
<tr>
<td>Figure 3.4</td>
<td>Home page for the 2 companies (Low Privacy Assurances condition)</td>
<td>74</td>
</tr>
<tr>
<td>Figure 3.5</td>
<td>Structural model. Dotted paths are non-significant</td>
<td>84</td>
</tr>
<tr>
<td>Figure 4.1</td>
<td>The Research Model</td>
<td>105</td>
</tr>
<tr>
<td>Figure 4.2a</td>
<td>Personal Control, High and Low levels</td>
<td>116</td>
</tr>
<tr>
<td>Figure 4.2b</td>
<td>Proxy Control, High and Low levels</td>
<td>116</td>
</tr>
<tr>
<td>Figure 4.2c</td>
<td>Collective Control, High and Low levels</td>
<td>117</td>
</tr>
<tr>
<td>Figure 4.2</td>
<td>Structural Regression Model Results</td>
<td>125</td>
</tr>
<tr>
<td>Figure 4.3</td>
<td>Alternative models considered</td>
<td>126</td>
</tr>
</tbody>
</table>
CHAPTER 1

INTRODUCTION

1.1 Online Privacy and Privacy Concerns in IS Research

Information Systems (IS) research has dedicated ample attention to issues of privacy. Whereas a few decades ago, the communication of information was done mainly via paper forms, today, the vast majority of all information transactions are carried out electronically. Not only is technological medium currently favored for information transmission, but it has itself become the reason why the amount of personal information has increased enormously: “Personal information in a digital format can be easily copied, transmitted, and integrated, which enables online marketers to construct thorough descriptions of individuals. Therefore, this information could pose a serious threat to privacy if not properly handled” (Malhotra, Kim, & Agarwal, 2004). Hence, privacy is an issue of mutual interest for companies and individuals alike.

One of the first, and most commonly used, privacy constructs in IS is privacy concerns (J. Smith et al., 1996). Ever since its introduction, this construct has served as the default conceptualization and measure of privacy in the field (Miltgen & Peyrat-guillard, 2014). Privacy concerns was proposed as a second-order construct made up by the four dimensions of collection, errors, unauthorized access and secondary use. A second important conceptualization is the Internet Users’ Information Privacy Concerns, (IUIPC) (Malhotra et al., 2004). Designed with an internet setting in mind, IUIPC is also proposed as a second-order construct which includes the three dimensions of collection, control and awareness of privacy practices. Yet a third mention-worthy construct,
Internet Privacy Concerns (IPC) (Hong & Thong, 2013), reverts back to Smith’s original four-dimensional model and adds the two from (Malhotra et al., 2004). In this conceptualization, the IPC is proposed as a third-order construct with two intermediate subdimensions and six first-degree dimensions of collection, errors, unauthorized access, secondary use, control and awareness. Even though the Hong & Thong (2013) conceptualization updates a nearly 20-year-old model, studies of privacy to this day tend to apply Smith’s parsimonious model over the newer Malhotra et al. (2004) and Hong & Thong (2013) conceptualizations.

An important consideration of privacy research in Information Systems (IS) is that of information sensitivity. Information sensitivity describes how individuals react differently regarding their privacy needs depending on the subject matter of the information at hand. For instance, financial and medical information may be perceived as inherently more ‘private’ realms of information than others. While some research acknowledges the importance of information sensitivity in the context of privacy (Bansal, Zahedi, & Gefen, 2010; Dinev, Xu, Smith, & Hart, 2013), little research has examined the effects of information sensitivity on privacy concerns and risk. Researchers have also noted that “future research on information privacy tools and techniques should likewise be more contextually sensitive.” (Belanger & Crossler, 2011).

The privacy literature in IS has given limited attention to information sensitivity, as the vast majority of studies focus exclusively on the type of information typically transacted in e-commerce settings. However, as internet communications evolve, other types of information are typically exchanged nowadays which begs the specific analysis of the actual sensitivity of the information. Modern technology applications such as
social media and online community platforms may present a newer, more specific setting to better illustrate and define boundaries in the privacy research. A particular case for this comes from online health communities (OHCs) where individuals exchange personal, health-related information. These special types of social networks offer researchers the opportunity to have a detailed view of the mechanics of privacy in a setting which showcases information sensitivity in a true-to-life context.

The constructs applied in the study of IS privacy have not seen a lot of evolution in the last couple of decades. Inconclusive results found in the privacy literature (e.g., Lowry et al., 2012) may also provide a fertile ground for researchers to employ newer measures and different research methods. The concept of control may provide this opportunity, since the control construct is intrinsically entangled with the notion of privacy (Belanger & Crossler, 2011), yet not many of the empirical studies of privacy have measured the degree of control given to individuals or its subsequent effects in the privacy phenomena. More specifically, the inclusion of control constructs in privacy research, under the light of new, control-focused theoretical frameworks, represents a clear research opportunity.

Privacy research has relied on several theories in the past, including but not limited to the Theory of Reasoned Action (TRA) (Ajzen & Fishbein, 1975), the Theory of Planned Behavior (TPB) (Ajzen, 1991), and the IS-native theory, Privacy Calculus (Dinev & Hart, 2006), which is more commonly employed in IS studies of privacy. However, theories that offer a richer view of the role of control are yet to be widely explored. The agentic perspective of social cognitive theory (Bandura, 2001) offers a newer approach which describes three different types of control (human agency) that can
be appropriately applied to the understanding of online privacy. In a 2012 experimental study, Xu et al., (2012), manipulated personal and proxy control, based on the agentic perspective, to examine privacy in the context of a location tracking service. However, the third type of control (collective) as described by the theoretical framework (agentic perspective) was not included in this study. Incorporating all three types of control in a privacy study would offer researchers the possibility to widen our understanding of online privacy and further knowledge about the role of control in privacy with online communities.

In an effort to address the above-described research opportunities, the following research questions are presented and are the focus of this dissertation document:

1. How widely has the concept of privacy been studied in the online health community setting and in online settings in general?

2. Which are the most prevalent antecedents, privacy-related constructs, and outcomes in the online privacy-related IS research?

3. What knowledge gaps exist in the literature that may further the understanding of privacy in online health communities?

4. How do control, privacy assurances and information sensitivity influence specific forms of privacy concerns and common outcomes?

5. How do different types of control affect the impact of privacy concerns on the formation of risk, trust, and intention to disclose information?
1.2 Organization of the Dissertation Manuscript

Chapter 2 presents an in-depth literature review of online privacy and identifies the research trends with a focus on online communities and more specifically online health communities. The literature review explores the chronology and evolution of the major trends in the study of privacy and specifically follows the development of important privacy-related constructs. A nomological network of online privacy informs the depth and breadth in which different constructs have been studied and it unveils research gaps that may be exploited. Chapter 2 addresses research questions 1 through 3 above: (1) How widely has the concept of privacy been studied in the online health community setting and in online settings in general? (2) Which are the most prevalent antecedents, privacy related constructs and outcomes in the online privacy-related IS research? And (3) What knowledge gaps exist in the literature that may further the understanding of privacy in online health communities?

Chapter 3 presents an empirical study that examines privacy assurances with varying levels of information sensitivity and information sharing control to better understand privacy concerns and other privacy-related outcomes. This study helps the researchers understand how different artifact characteristics, the degree of control an individual has over the management of their information, as well as the type of information being transacted can affect an individual’s privacy concerns, and his or her subsequent intention to disclose personal information to a web service provider. The privacy calculus model (Dinev & Hart, 2006) is used as the theoretical basis for the study which incorporates other important constructs in the literature such as trust, risk and the personal internet interest. Chapter 3 of this dissertation answers research question #4
above: How do control, privacy assurances and information sensitivity influence specific forms of privacy concerns and common outcomes?

Chapter 4 of this dissertation introduces a second empirical study adopting an innovative control conceptualization in the formation of individual-level privacy. Different types of control, according to the agentic perspective of social cognitive theory (Bandura, 2001), are measured in an experimental setting for their impact on important privacy-related constructs such as risk, trust and intention to disclose information. Chapter 4 specifically addresses question #5 in the preceding section: How do different types of control affect the impact of privacy concerns on the formation of risk, trust, and intention to disclose information?

The findings from the three dissertation papers, (chapters 2-4), have important theoretical and practical implications. A first important theoretical implication resides in the fact that antecedents to privacy, privacy assurances in the form of IT artifact characteristics, information sensitivity, and control, are operationalized in novel and meaningful ways. Second, these antecedents are incorporated into the privacy paradox model, a major IS theoretical framework, which is empirically tested and applied in a new context. Third, control is operationalized at three levels based on the agentic perspective of social cognitive theory and provides insight into how control over information can be offered to online users. Fourth, a comprehensive examination of multiple control levels and privacy-related outcomes was tested in an online health community context. Fifth, an empirical examination of the relationships among privacy-related outcomes was conducted in two different contexts, and provides insight into how risk, trust and intention to disclose information are formed and related.
As for implications for practitioners, first, the online artifact can present control tools which are demonstrated to have a significant effect on users’ intention to disclose information and participation in online communities. Second, privacy assurances as characteristics of a website are shown to have influence over trust and practitioners may use these to enhance their customers’ trust towards the site. Third, the inclusion of control tools into online communities is also an efficient way to ensure participation and disclosure in these communities. Fourth, evidence for the combined effect of control and privacy assurances on the individual degree of trust is provided which can be useful in settings where the exchanged information may be seen as inherently sensitive. Finally, the concluding chapter of this dissertation discusses several future research directions that build on this work and layout a path for expanding the knowledge of privacy in information systems.
CHAPTER 2

LITERATURE REVIEW

PRIVACY IN ONLINE HEALTH COMMUNITIES

2.1 Introduction

Privacy issues appear on a daily basis in the news media: Data leaks in prominent organizations; cultural and social issues around people’s rights to privacy; policy conflicts related to privacy, such as the Internet Freedom Act, or large corporations filtering individuals’ access to information, among many others. The healthcare field is no exception to this phenomenon, particularly in today’s world when having access to timely and complete information is a matter of life and death during a global pandemic. Further, healthcare providers and organizations in the United States have a legal mandate to protect patient’s healthcare privacy. The Federal Health Insurance Portability and Accountability Act (HIPAA), along with the Omnibus rule, provide clear specifications on what constitutes proper protection of personal health information and outline mandatory procedures for securing such information from inappropriate use or access (Kho et al., 2015). Thus, privacy concerns, in general, and specifically in healthcare, are an important research area that continues to grow in relevance, with broad implications for many aspects of our lives.

At the same time, the widespread use and popularity of internet technologies has brought about a myriad of enhancements to traditional business functions. A specific setting in which technology has had a powerful influence in the healthcare field is what is known as online health communities (OHCs). OHCs are websites and social networking
sites that have gained popularity among patients and general users alike, who wish to procure information relevant to their personal health conditions (Munson et al., 2013). OHCs offer expanded social learning opportunities for individuals with chronic illness through social support, knowledge exchange, and data sharing (Vaala et al., 2017). The use of these sites is, however, not without potential downsides. In these settings, the source of the information is the patient and therefore, the regulation of the content is not constrained by federal mandates. While healthcare providers are subject to privacy regulations, these requirements do not apply to individuals who are the owners and responsible parties for the security of their own information. They, the individual/patient, may opt to contribute (or not) their personal health information. Such contributions represent the wealth of knowledge that patients are afforded by these tools. Therefore, maximizing these contributions while helping patients manage their privacy and security effectively, presents a contentious argument for the study and analysis of privacy in an online healthcare context.

Understanding privacy is vital for the internet era-organization. As more services move to the internet, encouraging and guaranteeing the safe adoption of internet technologies becomes a pressing need for modern organizations. One of the most prevalent deterrents of internet adoption deals with issues of privacy (Boonstra & Broekhuis, 2010). In a national survey conducted in 2011, nearly half of the participants (48%) stated that they believe the Health Information Exchange (a platform to share patient information among health providers) will result in worsening of the privacy and security of their personal information (Ancker et al., 2013). The privacy of OHCs’ users may be compromised in many ways within these online communities and technologies (J.
Li, 2015). Personal health information (PHI) is often freely available within OHCs and represents a special type of information regarded as highly sensitive by individuals. In OHCs, personal health information is exposed to the scrutiny of members of these communities and can fall prey to data mining efforts by individuals and organizations seeking to monetize it (Belanger & Crossler, 2011; Dinev et al., 2013; Yu et al., 2015). PHI can also be compromised due to data misuses, disclosures to intruders, accidental data releases, disclosures to third parties and apps, and user profiling across multiple social networks (J. Li, 2015).

This present literature review focuses on the study of privacy in online health communities and aims to address the following research questions:

1. How widely has the concept of privacy been studied in the online health community setting, and in online settings in general?

2. Which are the most prevalent antecedents, privacy-related constructs, and outcomes in online privacy-related research?

3. What knowledge gaps exist in the literature that may further the understanding of privacy in online health communities?

In the following sections, a brief review of the privacy literature is provided in advance of introducing the formal method and results of a literature search for empirical studies of privacy in IS and healthcare journals. Based on this literature search and review, gaps in privacy research are identified and future research opportunities are discussed.
2.2 Literature Review: Privacy and online health communities

In the following sections, seminal research, theory, and background information on privacy and online health communities is described. This discussion provides a foundation and history on these two research areas, which informs the formal empirical literature search and review that is conducted.

2.2.1 Privacy

One of the most widely adopted views of privacy comes from (Warren & Brandeis, 1890), as quoted by (Dinev et al., 2013), which defines privacy as the right of the individual to be left alone or, that is, the right for isolation. This view on privacy has been adopted as the standard in law disciplines. In a more modern approach, privacy has been conceptualized as the control of the information (Margulis, 1977; Westin, 1967) which is the basis for the privacy interpretations commonly adopted in information systems. Another relevant conceptualization is that of information privacy which is yet a more novel take on privacy studies. Information privacy has been defined as the “ability of the individual to personally control information about one’s self” (J. Smith et al., 1996), and is the focus of this, and subsequent chapters. For the remainder of this dissertation proposal document, the term privacy is meant to refer to information privacy. Further, online information privacy is meant to refer to the ability of an individual to control his or her own personal information within an online context.

Privacy, as illustrated by several works, is a complex concept (Dinev et al., 2013; Hong & Thong, 2013; Margulis, 1977). Its complexity stems from its far-reaching connotations of social importance. A clear illustration of this comes from the seminal
work of Laufer & Wolfe, (1977) in which the authors explain: “…privacy is a catchall concept incorporating a multitude of meanings and evoking a wide range of human emotions. Privacy as it touches the unknowable is fraught with danger; as it promises mutuality and sharing, it touches profound needs; as it threatens exclusion, it raises fears.” Privacy has been chosen as the central construct of this study for it captures all the nuances and history as well as different applications that can potentially inform this analysis.

Studies of privacy have traditionally focused on external threats to privacy but much fewer have studied the owner of the information as the source of this threat (van der Velden & Emam, 2013). Individuals sharing their personal information is one of the most important reasons why privacy violations occur. This study focuses on the individual level of privacy for two reasons: First, Personal Health Information (PHI) in the context of online health communities is inherent to the individual patient/user. Second, past studies have defined privacy as one’s ability to control information about themselves (Belanger et al., 2002; E. F. Stone & Stone, 1990). It is precisely the risk of losing control of personal information that makes privacy a prevalent issue in the IS and healthcare fields.

Privacy concerns and privacy risks are two frequently studied privacy-related constructs in IS research, and have been studied as antecedents, mediators, moderators and outcomes. As evidenced by the theoretical framework developed by Y. Li, (2012), a considerable body of literature considers both perceived privacy risks and privacy concerns as highly related or even the same concept. However, several articles utilize both constructs within the same study (Andrews et al., 2014; Bansal et al., 2010; Dinev et
al., 2006; Miltgen & Smith, 2015) demonstrating that there are notable differences between them. From the perspective of this dissertation proposal, we adopt the Malhotra et al., (2004) definition which proposes that privacy concerns are individuals’ inherent worries about possible loss of information privacy. Alternatively, privacy risks is defined as the expectation that a high potential for loss is associated with the release of personal informal (Posey et al., 2010). Thus, perceived privacy risks are considered a distinct construct and an antecedent to privacy concerns (Andrews et al., 2014; Bansal et al., 2010; Miltgen & Smith, 2015). The internalization/cognitive adoption process of individuals results in these risks being converted into privacy concerns. The following paragraphs provide the reader with background and historical information about these two important constructs to provide some context for this review.

Privacy concerns (PC) has been utilized as the proxy construct for studies of privacy (Dinev et al., 2013; Miltgen & Peyrat-guillard, 2014). As a concept, privacy concerns was born out of the work by J. Smith et al., (1996) proposing that PC is a second degree, five-factor construct consisting of: collection, errors, external unauthorized secondary use, internal unauthorized secondary use and improper access. This construct has allowed the IS field to avoid the innate difficulties of the privacy conceptualization and focuses on measurable constructs that have been repeatedly validated as proper dimensions of privacy. The original framework (J. Smith et al., 1996), consisting of five elements of information privacy, is described below:

1. Collection of personal information: the amount of data being requested from individuals.
2. Internal unauthorized secondary use of personal information: the usage of information within the organization it was provided to by members not being authorized to handle it.

3. External unauthorized secondary use of personal information: the usage of information outside the organization it was meant for.

4. Errors in personal information: the degradation of actual information contained in the files resulting in inaccurate data.

5. Improper access to personal information: the malicious or commercial access and usage of the information without the consent of the individual.

The original measurement instrument was a Likert-type 15-item scale. Since its inception, the construct and scale have been modified and tweaked, and its most widely used variation today measures four constructs, merging internal and external unauthorized use of personal information. Its subsequent wide adoption makes privacy concerns the most important construct in the IS privacy literature. The Smith et al. (1996) construct was not designed for studies of privacy on the internet, and was instead, a scale development effort which included no IT artifact. Subsequent adaptations of this scale have been made to address online privacy concerns.

A second noteworthy construct in the literature is privacy risk, or perceived privacy risk (Van der Heijden et al., 2003), and can be understood as the subjective magnitude of adverse consequences and the probabilities that loss may occur (Dowling & Staelin, 1994). More aptly defined in specific terms for the online communications setting, (Dinev & Hart, 2006) explained perceived privacy risks as “a perceived potential risk that occurs when personal information is revealed” (pp. 394). An early scale to
measure perceived privacy risk was developed by Jarvenpaa & Tractinsky, (1999), which has since been widely adapted and changed through different studies for context-specificity and for contemporary applications/technologies.

It is also important to recognize the relevance of privacy with regards to its novel nature. Junglas, Johnson, & Spitzmüller, (2008) state that privacy coevolves with technology, and technology is ever-changing so it is expected that privacy matters will be a source of research opportunities as new technologies evolve and displace old ones. All of the empirical articles documented in this literature review happen to be published since 2002, which shows how contemporary and relevant the topic is in modern IS research.

2.2.2 Theory in Privacy Research

Theoretical perspectives considered in privacy research include the theory of reasoned action (TRA) (Liu et al., 2005), the privacy paradox (Dinev & Hart, 2006), the elaboration likelihood model (Bansal et al., 2015), and the agentic model (Xu et al., 2012). TRA has been applied to IS privacy research to explain how privacy-related beliefs can influence the behavioral intention to disclose personal information (Bansal et al., 2016; Liu et al., 2005; Lowry et al., 2011). The privacy paradox provides additional insight into behavioral intention to disclose personal information by considering beliefs as a set or collection of beliefs which are evaluated through a decision process or calculus. Several studies have utilized the privacy paradox to explain the cost-benefit analysis that individuals make when deciding whether to disclose personal information (Dinev et al., 2006, 2013; Jiang et al., 2013; Kehr et al., 2015; Kordzadeh & Warren, 2017). ELM has been applied in IS privacy research to provide insight in the more specific context of when privacy assurances are provided and these assurances can
function like peripheral cues influencing attitudes through automatic processing (Angst & Agarwal, 2009; Bansal et al., 2015; Gu et al., 2017). Recently, the agentic perspective of social cognitive theory (Bandura, 2001) has been applied to better understand privacy control (Xu et al., 2012). The agentic perspective distinguishes among three modes of agency: direct personal agency, proxy agency, which relies on others to act in one's behest to secure desired outcomes, and collective agency exercised through socially coordinative and interdependent effort. This theoretical perspective holds promise for better understanding how different levels of control may influence privacy concerns related behavior.

2.2.3 Online Health Communities

The study of privacy in OHCs is of special interest to the IS field for two prevalent reasons:

1. OHCs are a newer form of online technology that supports the transmission of information for many participants, using the internet and social media sites.

2. Privacy in an online healthcare context may have greater information sensitivity and risk than other contexts due to the nature of the information being shared, which may hinder the adoption and use of OHCs.

Known by names such as health social networking sites, (J. Li, 2015) health information systems or online patient communities (J. H. Frost & Massaglia, 2008), online health communities are virtual communities where users connect with each other around common problems and share relevant health data (J. Li, 2013). For this analysis, online health communities comprise all internet-enabled tools that can help patients connect to
others and share their health-related experiences, feelings, information, or ideas with others. These include health-specific sites such as Patients Like Me (https://www.patientslikeme.com/); forums of general or specific interest such as Reddit or Diabetes Daily (https://www.reddit.com/r/diabetes/; https://www.diabetesdaily.com/) and general social networking sites where health related information is exchanged within interest groups such as Facebook (https://www.facebook.com/) (Munson et al., 2013).

In online health communities, it is precisely the exchange of the information about individuals that may pose a risk to the user’s privacy. Researchers have argued that PHI is particularly sensitive to issues of privacy: “between 15% and 17% of US adults have changed their behavior to protect the privacy of their health information, doing things such as: going to another doctor, paying out-of-pocket when insured to avoid disclosure, not seeking care to avoid disclosure to an employer, giving inaccurate or incomplete information on medical history, self-treating or self-medicating rather than seeing a provider, or asking a doctor not to write down the health problem or record a less serious or embarrassing condition” (Malin, Emam, & O’Keefe, 2013). A different study showed that 13% of the respondents indicated having a health provider who uses an electronic health record and this caused them to withhold health-related information from their providers (Campos-castillo & Anthony, 2015).

Social networks, and specifically OHCs represent an important setting for the study of privacy. The mechanism of communication, the governance of privacy or site-specific policies (privacy assurances), the purpose, the audience, among other unique factors demonstrate that it constitutes a very specific environment in which privacy plays an important role. Given the importance of studying privacy in general, and specifically
in an online health community context, a formal literature review was conducted to identify and examine empirical studies of privacy concerns in an online context. The goal of this literature review is to better understand the existing research on privacy concerns and to identify gaps in the literature that would benefit from further theoretical and empirical examination.

### 2.3 Methodology

The following section provides a detailed description of the methodology utilized for the identification of potentially relevant journals and articles. The search terms and other filters used to identify relevant articles within these journals are also described. A list of all queried journals, as well as a description of the search process is provided.

#### 2.3.1 Journal Selection

The consulted journals are from both the information systems as well as the healthcare technology fields. Table 2.1 presents a list of the seventeen journals selected for this study. The journals selected from information systems were those listed by the Association of Information Systems (AIS) in their website (http://aisnet.org/?SeniorScholarBasket) as the senior scholars’ basket of journals. The selected healthcare technology journals included the most representative journals listed in the AIS SIG-Health group’s website. The SIG Health is a special interest group of researchers within AIS whose focus is the health-related realms of information systems. The list of journals is a compilation of the journals reported by SIG Health members in 2016 as those being most utilized in the past for their personal research projects. The top six journals on this list were selected for the search referenced in this paper. The list is
available at http://www.aissighealth.com/wordpress/health-is-journals/. Finally, all publications with a ranking of ‘A-‘ or above on the Isenberg IS journal list were also included in the search. This resulted in the addition of three journals, bringing the total number of journals to seventeen.

Table 2.1 - List of consulted journals & search stage

<table>
<thead>
<tr>
<th>Journal</th>
<th>Acronym</th>
</tr>
</thead>
<tbody>
<tr>
<td>European Journal of Information Systems</td>
<td>EJIS</td>
</tr>
<tr>
<td>Information Systems Journal</td>
<td>ISJ</td>
</tr>
<tr>
<td>Information Systems Research</td>
<td>ISR</td>
</tr>
<tr>
<td>Journal of AIS</td>
<td>JAIS</td>
</tr>
<tr>
<td>Journal of Information Technology</td>
<td>JIT</td>
</tr>
<tr>
<td>Journal of Management Information Systems</td>
<td>JMIS</td>
</tr>
<tr>
<td>Journal of Strategic Information Systems</td>
<td>JSIS</td>
</tr>
<tr>
<td>Management of Information Systems Quarterly</td>
<td>MISQ</td>
</tr>
<tr>
<td>International Journal of Medical Informatics</td>
<td>IJMI</td>
</tr>
<tr>
<td>Decision Support Systems</td>
<td>DSS</td>
</tr>
<tr>
<td>Decision Sciences</td>
<td>DS</td>
</tr>
<tr>
<td>Information &amp; Management</td>
<td>I&amp;M</td>
</tr>
<tr>
<td>Journal of the American Medical Informatics Association</td>
<td>JAMIA</td>
</tr>
<tr>
<td>Journal of Medical Internet Research</td>
<td>JMIR</td>
</tr>
<tr>
<td>Journal of Medical Systems</td>
<td>JOMS</td>
</tr>
<tr>
<td>Health Policy and Technology</td>
<td>HPT</td>
</tr>
<tr>
<td>International Journal of Medical Informatics</td>
<td>IJMI</td>
</tr>
</tbody>
</table>
2.3.2 Article Selection

Each journal was queried utilizing a database search engine such as ABI Inform Complete, ProQuest or Business Source Complete with these being favored (in that particular order) to any others when more than one was available via the UMASS libraries system. The search criteria within each publication was whether the word “privacy” was contained in the abstract of the article. This search produced a total of 508 articles. Among those, the selected papers had to meet four distinct criteria:

1. Article included an empirical study,
2. Article included an empirical measure of a privacy-related construct,
3. The study was conducted at the individual level of analysis.
4. The study examined an online health community, or an online context similar to OHC.

Every article was analyzed at the abstract level to ensure they met the selection criteria. If the abstract couldn’t provide the necessary information to make a selection decision, a review of the entire article was conducted. A total of 455 articles were excluded for not meeting the above-described criteria and a resulting total number of fifty-three articles were finally selected for this analysis. Most of the exclusions were the result of articles not including an empirical measure of a privacy-related concept. Of the fifty-three meeting the selection criteria, only four come from the medical technology literature. Many of the articles from the medical technology journals are either editorial or descriptive in nature with no empirical study included. Further, the medical technology field is largely interested in the institution-level roles and responsibilities related to privacy. Privacy is often mentioned in the abstract of such studies only as pertaining to its
relationship to information security (Andrews et al., 2014). Most of the retained articles from the IS journals were not related to the specific context of OHCs. Given the newness of the topic, there were few empirical articles on OHC, but similar studies of online privacy were relevant to the present study given the focus on privacy, the central construct in the present study. All selected articles involve the presence of an online artifact comparable to an OHC. An artifact is a technology ‘device’ that is present in the activity at hand. In the OHC setting, the artifact would be the tool itself: the social network or website. Due to this extension, two other salient contexts/settings arise in the selected articles: E-commerce and Social networks.

In the next section, a list of the selected empirical articles and a discussion of the articles is provided. The discussion addresses the privacy constructs examined in each article and summaries of article findings, as well as short notes of observations and an integrated nomology of the empirical articles reviewed.

2.3 Discussion of Empirical Studies

The discussion of results from the review of 53 empirical studies is organized as follows. First, privacy-related constructs are discussed with Table 2.2 providing a listing of the 53 articles, including the privacy-related construct(s) measured in each study, a reference number used in charts and other tables to direct the reader to the relevant articles, and whether the construct is studied as an endogenous variable (in the case of mediators, moderators or outcomes) or an exogenous one (for antecedents). Next, a short discussion of four notable exceptions to this taxonomy is presented. Then, the articles reviewed in which privacy-related constructs are antecedents are described. Next, articles reviewed in which privacy-related constructs serve as outcomes are then described and
organized based on the antecedents to these privacy-related constructs (i.e., internal antecedents: personality traits, perceptions/beliefs, and external antecedents: artifacts and contexts). There are a few articles in which privacy-related constructs serve as both antecedents and outcomes within a research model (i.e., moderators/mediators), and those articles are described in both the antecedent (exogenous) and outcomes (endogenous) sections. Finally, the outcomes of privacy-related constructs are described in more detail before a nomological model of antecedents and outcomes to privacy-related constructs is presented.

Table 2.2 - Privacy-related constructs in the literature.

<table>
<thead>
<tr>
<th>#</th>
<th>Author(s)</th>
<th>Year</th>
<th>Privacy related construct</th>
<th>Endo/Exo</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Bansal, Zahedi &amp; Gefen</td>
<td>2010</td>
<td>Information privacy concern; Risk beliefs</td>
<td>Endogenous</td>
</tr>
<tr>
<td>2</td>
<td>Midha</td>
<td>2012</td>
<td>Consumer privacy empowerment</td>
<td>Exogenous</td>
</tr>
<tr>
<td>3</td>
<td>Li</td>
<td>2014</td>
<td>Privacy concerns</td>
<td>Endogenous</td>
</tr>
<tr>
<td>4</td>
<td>Gu, et. al</td>
<td>2017</td>
<td>Privacy concern</td>
<td>Endogenous</td>
</tr>
<tr>
<td>5</td>
<td>Mousavizadeh, Kim &amp; Chen</td>
<td>2016</td>
<td>Privacy concerns</td>
<td>Endogenous</td>
</tr>
<tr>
<td>6</td>
<td>Dinev, et. al</td>
<td>2006</td>
<td>Privacy concerns, privacy risks</td>
<td>Endogenous &amp; Exogenous</td>
</tr>
<tr>
<td>7</td>
<td>Pose, et. al</td>
<td>2010</td>
<td>Privacy risk belief</td>
<td>Exogenous</td>
</tr>
<tr>
<td>8</td>
<td>Dinev, et. al</td>
<td>2013</td>
<td>Perceived privacy</td>
<td>Endogenous</td>
</tr>
<tr>
<td>9</td>
<td>Bansal, Zahedi &amp; Gefen</td>
<td>2015</td>
<td>Privacy concerns</td>
<td>Endogenous</td>
</tr>
<tr>
<td>10</td>
<td>Miltgen &amp; Peyrat-Guillard</td>
<td>2014</td>
<td>Privacy concerns</td>
<td>Endogenous</td>
</tr>
<tr>
<td>11</td>
<td>Li &amp; Unger</td>
<td>2012</td>
<td>Privacy concerns</td>
<td>Exogenous</td>
</tr>
<tr>
<td>12</td>
<td>Pramatari &amp; Theotokis</td>
<td>2009</td>
<td>Privacy concern</td>
<td>Exogenous</td>
</tr>
<tr>
<td>13</td>
<td>Junglas, Johnson &amp; Spitzmuller</td>
<td>2008</td>
<td>Concern for privacy</td>
<td>Endogenous</td>
</tr>
<tr>
<td>14</td>
<td>Sato &amp; Costa-i-Font</td>
<td>2013</td>
<td>Privacy of personal information; Perceptions of privacy</td>
<td>Exogenous</td>
</tr>
<tr>
<td>15</td>
<td>James, et. al</td>
<td>2017</td>
<td>Concern for information privacy</td>
<td>Exogenous</td>
</tr>
<tr>
<td>16</td>
<td>Li, et. al</td>
<td>2016</td>
<td>General privacy concern; Perc. Privacy control</td>
<td>Exogenous</td>
</tr>
<tr>
<td>17</td>
<td>Choi &amp; Land</td>
<td>2016</td>
<td>General privacy concerns; Transaction privacy concerns</td>
<td>Endogenous &amp; Exogenous</td>
</tr>
<tr>
<td>18</td>
<td>Bansal, Zahedi &amp; Gefen</td>
<td>2016</td>
<td>Internet privacy concern</td>
<td>Endogenous &amp; Exogenous</td>
</tr>
<tr>
<td>19</td>
<td>Li, Lin &amp; Wang</td>
<td>2015</td>
<td>Privacy disclosure behavior</td>
<td>Endogenous</td>
</tr>
<tr>
<td>20</td>
<td>Miltgen &amp; Smith</td>
<td>2015</td>
<td>Privacy risk concern</td>
<td>Endogenous</td>
</tr>
<tr>
<td>21</td>
<td>Ku, Chen &amp; Zhang</td>
<td>2013</td>
<td>Privacy concern</td>
<td>Exogenous</td>
</tr>
<tr>
<td>22</td>
<td>Schwaig, et. al</td>
<td>2013</td>
<td>Concern for Information privacy</td>
<td>Endogenous</td>
</tr>
<tr>
<td>23</td>
<td>Liu, et. al</td>
<td>2005</td>
<td>Privacy concerns</td>
<td>Exogenous</td>
</tr>
</tbody>
</table>
2.4.1 Focal Privacy-Related Constructs

In categorizing focal privacy constructs, constructs with slightly different names but similar operationalizations within each study were categorized together. For example, in the case of privacy concerns, some authors refer to it as concerns for privacy, information privacy concerns, or general privacy concerns. While the name or
operationalization may have varied slightly from study to study, the general notion stems from the Smith et al., (1996) definition of the construct, and thus these constructs are described under the general term of privacy concerns. The same criteria was applied to other similarly worded constructs such as perceived privacy risk, privacy risk belief and privacy risk concern, which are described under the general term of privacy risk.

The single most utilized privacy-related construct in the reviewed articles is privacy concerns, with the majority of the articles including privacy concerns (41 out of 53). Privacy concerns was previously defined as individuals’ inherent worries about possible loss of information privacy (Malhotra et al., 2004). In 21 articles, privacy concerns served as an antecedent (exogenous variable) in the research model and in 20 studies it served as a mediator/moderator or outcome (endogenous variable). This count is a testament to the widespread adoption of privacy concerns as the default construct for privacy in the information systems field (Dinev et al., 2006). Privacy risks (the high potential for loss is associated with the release of personal informal) was the next most commonly utilized constructs with nine articles, and four of those also included privacy concerns. In four articles, a variety of privacy-related constructs were studied, such as privacy, privacy behavior, displayed privacy information, etc.

The articles which examine privacy concerns are first discussed, and are organized in the following order: privacy concerns as antecedents to attitudes, intentions and finally, as antecedents to a behavior. This order was selected based on the categories of outcomes in the Theory of Reasoned Action (TRA). TRA proposes attitudes, intentions, and behavior in a sequential order (Lowry et al., 2011), with attitudes being defined as a summary evaluation of an individual of a specific item (Nelson T. D., 2017).
It is therefore intuitive to understand how they would in turn inform intentions, which are more of a plan or devise to do something, whereas carrying out such plan or acting accordingly to this plan would be considered a behavior. Articles that examine privacy risks and other privacy-related constructs are then discussed.

Of the total 53, four (4) articles cannot fit this taxonomy. Two studies were designed to validate and analyze the privacy concerns construct in isolation, with no antecedents or outcomes. These are the (Hong & Thong, 2013) article and the (Stewart & Segars, 2002) study. While Stewart & Segars, (2002) examines and validates the Smith et. al., (1996) instrument as it was proposed originally, the Hong & Thong (2013) examines different dimensional structures of privacy concerns. It adds the dimensions of Control and Awareness and proposes privacy control as a third-degree construct with two second-order sub-dimensions and six dimensions. The remaining two exceptions are: K. Li, Lin, & Wang, (2015), which presents a panel data analysis study from social networks (SN) measuring the relationship of SN size & experience as well as blogging productivity in the individuals’ privacy disclosure at two different levels of information sensitivity; and Wakefield, (2013) survey study analyzing the role of affect on the users’ trust and privacy beliefs which ultimately affect the intention to disclose. These two do not use any of the major privacy constructs in the literature: privacy concerns and privacy risks.

2.4.2 Privacy Concerns

Of the 21 selected articles utilizing privacy concerns as an antecedent, 3 measure it as an antecedent to an attitude. Pramatari & Theotokis, (2009), showed that attitudes toward the use of Radio Frequency Identification (RFID) technologies are negatively impacted by information privacy concerns. In this cross-cultural study between Ireland
and Greece, they were interested in measuring attitudes and developed a model measuring three attitudinal categories. One interesting observation from their study is that only two measurement items were used and both are from the collection dimension of privacy concerns. The original scale developed by Smith et. al., (1996) included fifteen items and measured five different dimensions, including a 3-item measure of collection. Choi & Land, (2015) view privacy concerns at two distinct levels within the same study: their study measures general privacy concerns as an antecedent of specific, or what they call “transactional” privacy concerns. Set in an e-commerce context, Malhotra, Kim & Agarwal, (2004) contend that privacy concerns are the direct predecessors to both trust and risk beliefs. Their study proposes the Internet Users’ Information Privacy Concern (IUIPC) construct and is a milestone in the privacy research for the online era.

By far, the type of construct that has been most widely measured as an outcome of privacy concerns is intentions, with 14 articles measuring privacy concerns as an antecedent to a form of intention or willingness to perform a behavior, including intention or willingness to provide/disclose information. Three studies that measure privacy concerns as antecedents to intention to provide information are in a healthcare context (Anderson & Agarwal, 2011; J. Frost et al., 2014; Kordzadeh & Warren, 2017), and three are set in an e-commerce (online shopping) context (Dinev et al., 2008; Hui et al., 2007; H. Li et al., 2016). In all six studies, the relationship between privacy concerns and intention or willingness to provide information was significant. Among the studies measuring the intention or willingness to use/adopt a system, the study by T. Li & Unger, (2012) takes place in the e-commerce setting. The articles measured intention to adopt a technology tool/characteristic that facilitates online shopping, namely personalization.
The adoption of these technologies would allow the flow of information between the sites (vendors) and the users in a more streamlined fashion and tailoring to the person’s needs considering the individual characteristics (or personal information).

Crossler & Posey, (2017) study the adoption of an identity ecosystem which is described as “a user-centric online environment, a set of technologies, policies, and agreed upon standards that securely supports transactions ranging from anonymous to fully authenticated and from low to high value” (pp. 489). Their paper does not consider a specific setting or context, instead it analyzes the potential to secure personal information in a setting-independent tool that can be adopted across different online services. In a similar fashion, Lowry et al., (2011) study the adoption of a tool that can facilitate the sharing of personal information in social media platforms. They call it a self-disclosure technology. Both studies present the possibility of using an external tool that can be utilized on top of (or independently from) existing web technologies that can facilitate and secure the transmission of information. Both studies find that privacy concerns would in fact have an impact on the adoption of said technologies. Finally, the study by Awad & Krishnan, (2006) measures the willingness to be profiled for services and for advertising. Privacy concerns is shown to be a significant determinant for individual’s willingness to be profiled in both settings.

Angst & Agarwal, (2009) measure the intention to adopt electronic health records as a function of the individual privacy concerns. This article is especially relevant since it’s contextualized in the healthcare setting, representing the only study of privacy concerns as an antecedent to the adoption of a healthcare technology. Electronic health records have received wide attention by the healthcare field for its potential benefits in
the management of information, and what that would entail for the quality of healthcare. However, privacy concerns continue to have a negative impact on the adoption of electronic health records. Alternatively, Ku, Chen, & Zhang, (2013) view privacy concerns as a direct antecedent to the individuals’ intention of continuous use of a social networking site.

Four papers examine privacy concerns as an antecedent to behavior. Set in the context of social media, James, Wallace, Warkentin, Kim, & Collignon, (2017) found that concerns for information privacy is an effective predictor of privacy protection behavior. Measuring how Facebook users utilize the site’s privacy control settings, they were able to determine the effect of privacy concerns when mediated by the risk of information exposure. Son & Kim, (2008), proposed three potential behaviors as a result of privacy concerns: information provision, private action, and public action. Each of them is further divided into two specific types, for a total of 6 potential behaviors called information privacy-protective responses. These 6 responses are defined as a set of Internet users’ behavioral responses to their perception of information privacy threats that result from companies’ information practices. Their study examines six hypotheses with privacy concerns as a predictor of each of the six responses: 1) Refusal; 2) Removal; 3) Negative word of mouth; 4) Complaining directly to online companies; 5) Complaining indirectly to third party organizations; and 6) Misrepresentation. All of these specific behaviors were correlated with the existence of privacy concerns in individuals, except for misrepresentation. Huang, Goo, Nam, & Yoo, (2017) found a significant impact of privacy concerns on the intention to use smart tourism technologies, given that tourism technologies require personal information to personalize the products offered to the user.
Lastly, Tsai, Egelman, Cranor, & Acquisti, (2011) measured the purchasing behavior of participants as a function of the experimentally manipulated privacy information and the individual’s measured online privacy concerns.

### 2.4.3 Perceived Privacy Risks

Perceived privacy risk served as the focal privacy construct or an antecedent to privacy concerns in thirteen (13) of the selected articles. As described below, privacy risk has been examined as an antecedent to attitudes, intentions, and behavior. In a study of adoption of electronic personal health records in Australia, Andrews et al., (2014) studied the influence of perceived privacy risks on the attitude towards the adoption intention. In this study, the roles of trust and privacy concerns were measured as moderators of the relationship between privacy risks and attitude towards adoption intention. This survey-based study reported that perceived privacy risk was the second strongest explanatory variable in the model and support was also found for the moderating roles of trust and privacy concerns suggesting that government communications may help adoption by increasing trust and reducing privacy concerns. Bansal et al., (2010) measured perceived privacy risks as a mediator construct between previous online privacy invasion and trust in the health website. Trust, in turn, was studied as an antecedent to the intention to disclose health information.

Dinev & Hart, (2006) measured the direct effect of perceived privacy risks on the willingness to provide information online, as well as on internet trust and privacy concerns as mediators of that relationship. The model was supported, and in an extension of this study, Dinev et al., (2013) found that an individual’s perceived privacy risk is a direct antecedent of his/her perceived privacy. In a study by Posey et al., (2010),
perceived privacy risk was examined in a panel data analysis of actual utilization of
social media sites, and found to have a strong negative effect on disclosure in online
communities.

As previously mentioned, privacy risk has also been examined as an antecedent to
privacy concerns. Dinev et al., (2006), carried out a comparative analysis between the
cultures of the United States and Italy with regards to the importance of perceived
privacy risk as an indicator of both privacy concerns (as a mediator to e-commerce
utilization) as well as to e-commerce utilization directly. Both relationships were found to
be significant for both countries. Not only perceived privacy risks are found to influence
privacy concerns, but the relationship is also stronger for Italy than for the United States,
showing that culture does play a role in the relationship between perceived privacy risks
and privacy concerns. A similar finding was encountered in a cross-cultural experimental
analysis by Kehr et al., (2015) where perceived privacy risks are found to be a significant
predictor of privacy concerns. (Xu, Dinev, Smith, & Hart, 2011a) utilized a survey study
to measure perceived privacy risks as antecedent to privacy concerns in different website
settings including electronic commerce sites, social networking sites, financial sites, and
healthcare sites.

In sum, privacy risks were found to be antecedents of the following outcomes in
the extant literature:

- Privacy concerns (Dinev et al., 2006; Xu et al., 2011b)
- Intention (or willingness) to disclose personal information and personal health
  information (Dinev & Hart, 2006; Gerlach et al., 2015; Malhotra et al., 2004;
  Posey et al., 2010)
• Attitude towards adoption of technology and electronic health records (Andrews et al., 2014)
• Different variations of trust (Bansal et al., 2010)
• Perceived privacy (Dinev et al., 2013; Kehr et al., 2015)
• Protection behavior and regulatory preferences (Miltgen & Smith, 2015)
• Self-disclosure (Krasnova et al., 2010; Yu et al., 2015)

2.4.4 Other Privacy Focal Constructs

Privacy assurances and the related concepts of displayed privacy information and privacy dimensions are also represented as privacy focal constructs examined in the reviewed articles. (Bansal et al., 2015) defines privacy assurances as “mechanisms that directly or indirectly provide customers with assurances and guarantees that their private information will be protected and kept private by the website.” (pp. 625). This study, based on the elaboration likelihood model, viewed privacy assurances as peripheral cues and utilized websites’ reputation, company information, design appeal, and perceived information quality as proxies for privacy assurances (peripheral cues). These four cues were measured utilizing pre-existing scales on related concepts such as trust, reliability, credibility, and trustworthiness. Although their results showed various levels of significance (with one exception), it must be mentioned that the chosen operationalization of privacy assurances doesn’t appear to explicitly measure privacy, beliefs, or attitudes.

Tsai et al., (2011) and Hann, Hui, Lee, & Png, (2007) are two studies that have measured “displayed privacy information”. This construct is similar to privacy assurance for being a characteristic of the artifact that provides its user’s access to a description of
the privacy approach (or philosophy) of the organization. Such definition matches closely with this study’s interpretation of privacy assurances. Tsai et al., (2011), in an experimental study showed that displayed privacy information has a significant positive impact on the intention to purchase of an individual. Hann et al., (2007), also in an experimental setting, measured the impact of specification of privacy protection on motivation to provide information and found strong support in favor of a positive relation. However, in a field experiment study, (Hui et al., 2007) operationalized privacy assurances as privacy statements and privacy seals and found that although a privacy statement has a marginally significant effect, privacy seals were insignificant in their impact on the consumer disclosure of personal information.

While Bansal et al., (2015) and Hui et al., (2007) have raised some questions about the applicability of their findings to the study of privacy, a fourth study (Liu et al., 2005) utilized what they called “privacy dimensions”. Their description of privacy dimensions aligns with the conceptualization of privacy assurances in a similar fashion to the cases of Tsai et al. (2011) and Hann et al., (2007). In fact, to define choice (one of these dimensions) Tsai et al. (2011) utilize the word “assurance”. The four described dimensions (assurances) are: notice, access, choice and security. These dimensions are adopted from the Federal Trade Commission as ‘principles of privacy’ (Federal Trade Commission, 2000) which entities should strive for. This study, set in an e-commerce context, finds strong support for the claim that all four assurances have a significant effect in the trust an individual displays for an electronic commerce site and this, in turn, is a strong predictor of the intention to purchase from it.
Assurances, taken in general, can be interpreted as a wide, diverse set of aspects or characteristics of the artifact that communicate a sense of privacy to the user. Although the results from this group of papers offers different views on the effect of assurances, the evidence appears to tilt in favor of a positive relationship between assurances and measures of privacy. Given that privacy assurances are arguably a direct way in which organizations can communicate their stance on the management of their information, more research into assurances seems necessary. Having completed a review of privacy-related constructs and how these constructs function as antecedents (exogenous) within research models, the next section describes how privacy-related constructs can function as outcomes (endogenous variables). Specifically, the antecedents to privacy-related constructs, including privacy concerns and privacy risks, are described.

2.4.5 Antecedents to Privacy-Related Constructs

Across the articles analyzed in this study, a total of 86 antecedents (48 distinct) to privacy-related constructs were identified. A typology of internal and external antecedents to privacy arises from canvassing these constructs. Such classification has been utilized in the literature for a similar analysis (Xu et al., 2011a). Antecedents that reference the individual, such as individual perceptions, beliefs or personal characteristics are categorized as internal while antecedents that are characteristics of the setting or the artifact are categorized as external. Xu et al., (2011a) similarly categorized privacy policy as an external source and “disposition to value privacy (DTVP)” as an internal source of impact to privacy risk (pp. 812). To visualize this distinction, an “internal vs. external” classification chart was created, as shown in Table 2.3.
Additionally, the antecedents are sub-classified as follows: Internal sources are either personal characteristics or perception/beliefs, whereas the external sources have been subdivided between artifact characteristics or context characteristics. While personality traits would be considered a personal characteristic source, an attitudinal construct would be classified as a perception or belief. The difference between personal characteristics and perception/beliefs resides on the temporal dimension of these concepts: personal characteristics tend to be a more permanent description or depiction of the individual, and perceptions/beliefs are a cognitive state with regards to a specific subject of knowledge. Perceptions/beliefs can also be characterized as less rigid and more susceptible to change since they could potentially transform as new information becomes available and is processed by the individual.

On the other hand, external antecedents might be subclassified as either artifact or context characteristics. An artifact characteristic is a defined functionality or attribute of the technology being used to access the service. An external antecedent such as “privacy policy visibility” (the degree by which a privacy policy is readily available to a site user) would be classified as an artifact characteristic antecedent. Alternatively, “cultural characteristics” (national or societal characteristics) or “information sensitivity” (the nature of the information transmitted) would be considered a context characteristic antecedent. A context characteristic can be thought of as a descriptive attribute of the IS setting but not the actual IS tool being utilized. J. Frost et al., (2014) shows, among other findings, that users of online health communities are in general more willing to share information that is otherwise thought to be sensitive. This assertion supports the notion to utilize ‘context’ as a useful category for privacy antecedents.
A comprehensive list of all identified antecedents to privacy-related constructs, in the four sub-classes, is provided in Table 2.3. The numbers next to the concept references the study in which it was utilized, as listed in Table 2.2. A few clear observations are apparent from this table: First, external and internal privacy-related antecedents are well represented. However, characteristics of the individual, either at the personal characteristics or at the perception/belief level occur much more frequently in the literature when compared to external antecedents. Second, cultural antecedents, namely Collectivism, Individualism, or Information sensitivity, taken from the fourth column of the table, represent a minority of the studies. In the following sections, these antecedents to privacy concerns, privacy risks, and other focal privacy constructs are described.

2.4.5.1 Internal Antecedents of Privacy

The first subclassification of common antecedents to privacy in the reviewed articles is presented as the “internal antecedents”. With reference to the individual, the privacy-related construct can either be originating or pertaining to the individual center of the research or, external to the person. Constructs that can be characterized as “internal” are personal characteristics or beliefs innate to the individual. They are independent from the environment, context or artifact which is being used to communicate aspects of privacy. The following represent the internal constructs more often seen used in the literature and used as antecedents to a privacy-related construct.

2.4.5.1.1 Previous Privacy Invasion

Prior privacy invasion contributes to disutility (Bansal et al., 2010). In utilitarian terms, this would reduce the perceived value of the artifact in question. The first internal
antecedent of privacy to review is previous privacy invasions. Culnan, (1993) found that prior negative privacy experiences influence the attitudes towards the use and request of information in marketing. In an e-commerce setting, previous negative experiences have shown to result in a negative attitude towards the value of the online marketplace (P. A. Pavlou & Gefen, 2004). Used in four different studies in the present review, (Bansal et al., 2010; Bansal et al., 2016; Frost et al., 2014; Awad & Krishnan, 2006) the previous privacy invasion construct represents one of the most utilized personal characteristics as an antecedent to privacy.

Bansal et al. (2010) measured previous online privacy invasion as an antecedent to both privacy concerns and risk beliefs finding a significant impact on both. A different study, published in a medical technology journal, showed prior negative experience to have a strong negative effect on patients’ intentions to share personal health-related information (Frost et al., 2014). To measure prior negative experience, they used a scale adopted from a trust study (Song & Zahedi, 2007). Both of these studies (Bansal et al., 2010; J. Frost et al., 2014) were specifically applied in a healthcare setting which makes them especially relevant to this analysis. Bansal et al., (2016) later found that previous privacy invasion is also a significant antecedent to trust and intention to disclose personal information. In this multi-setting study, privacy concerns significantly mediated the relationship between previous privacy invasion and intention to disclose personal information.
Table 2.3 - Classification of antecedents to privacy-related constructs in the literature.

<table>
<thead>
<tr>
<th></th>
<th><strong>INTERNAL</strong></th>
<th></th>
<th><strong>EXTERNAL</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Pers. Characteristics</td>
<td>Perceptions/Beliefs</td>
<td>Artifact characteristic</td>
<td>Context Characteristics</td>
<td></td>
</tr>
<tr>
<td>Personality traits</td>
<td>Perceived information control</td>
<td>Consumer privacy empowerment</td>
<td>Information sensitivity</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(8, 16)</td>
<td></td>
<td>(1)</td>
<td></td>
</tr>
<tr>
<td>Experience</td>
<td>Perceived benefits of disclosure</td>
<td>Website reputation</td>
<td>Contextual cues</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(26)</td>
<td></td>
<td>(4)</td>
<td></td>
</tr>
<tr>
<td>Health status</td>
<td>Perceived anonymity of self</td>
<td>Anonymity</td>
<td>Individualism</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(29)</td>
<td></td>
<td>(7)</td>
<td></td>
</tr>
<tr>
<td>Prior privacy invasions</td>
<td>Perceived anonymity of others</td>
<td>Application privacy attributes</td>
<td>Collectivism</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(29)</td>
<td>(17)</td>
<td>(7)</td>
<td></td>
</tr>
<tr>
<td>Website familiarity</td>
<td>Perceived privacy control</td>
<td>Control</td>
<td>Country Culture</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(33, 38)</td>
<td></td>
<td>(10, 42)</td>
<td></td>
</tr>
<tr>
<td>Age</td>
<td>Expected community utility</td>
<td>Information accessibility</td>
<td>Environmental dimension</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(39)</td>
<td></td>
<td>(16)</td>
<td></td>
</tr>
<tr>
<td>Gender</td>
<td>Perc. need for gov. surveillance</td>
<td>Privacy Policy Permissiveness</td>
<td>Financial gain</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(47)</td>
<td></td>
<td>(41)</td>
<td></td>
</tr>
<tr>
<td>Personal social network</td>
<td>Importance of privacy policies</td>
<td>Personalization</td>
<td></td>
<td></td>
</tr>
<tr>
<td>size</td>
<td>(53)</td>
<td></td>
<td>(51)</td>
<td></td>
</tr>
<tr>
<td>Blogging productivity</td>
<td>Affective Commitment</td>
<td>Privacy-Safe attributes</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(35)</td>
<td></td>
<td>(51)</td>
<td></td>
</tr>
<tr>
<td>Regulatory knowledge</td>
<td>Trust in other members</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(38)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disposition to privacy</td>
<td>Trust in OSN provider</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(38)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interpersonal awareness</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Affect</td>
<td>(42)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trust indices</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Awareness</td>
<td>(43, 45)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(44)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(50)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Throughout the body of research analyzed, previous privacy invasion is consistently shown to be a significant predictor of privacy (privacy concerns, privacy risks, etc.). Given the number of studies which have validated this notion, and due to it having an intuitive relation, this construct should be utilized as an effective correlate to privacy in future research. Given the relative ease with which this construct can be measured (i.e. asking “have you had a prior privacy negative experience?”), it might have a place in research studies where a personal privacy or privacy concern correlate would be desired.

2.4.5.1.2 Personality Traits

A second, widely utilized internal antecedent to privacy is personality traits. Three different studies in this literature review have considered personality traits as antecedents to a form of privacy (Bansal et al., 2010, 2016; Junglas et al., 2008). All three articles have used either of two variations of a similar construct to measure personality traits: The Big-Five factor structure (Goldberg, 1990) or the NEO personality inventory (McCrae & Costa, 1987). This construct defines 5 dimensions of personality consisting of Openness (or Intellect), Conscientiousness, Extroversion (vs. Introversion), Agreeableness and Neuroticism (Emotional Instability). Since its inception in the late 80’s, early 90’s, the Big-Five factor structure has been the default measure of personality in the information systems field. Personality traits are “individual dispositional characteristics” that have been found to be relatively stable across individuals’ adult lifespan (Costa et al., 1991).
Junglas et al., (2008) studied the direct influence of Big-Five factor structure on concern for privacy. In this survey-based study, a test of structural model shows that agreeableness, conscientiousness and openness to experience are significant contributing factors to the formation of concern for privacy. In a more contemporary study, Bansal et al., (2010) tested the Big-Five factor structure as antecedent to perceived health information sensitivity, which was construed as the mediator leading to health information privacy concern. In other words, the personality indicator was an indirect antecedent to a privacy measure. The experimental study, set in the healthcare information setting, showed support for Intellect, Emotional Instability and Agreeableness as significant antecedents to perceived health information sensitivity. As noted, both studies show the same three (out of the five) factors to lead directly and indirectly respectively to a measure of privacy.

Based on the previous study finding support for Intellect, Emotional Instability and Agreeableness as formative measures of concern for privacy, Bansal et al., (2016) utilized those three factors exclusively for their study. In this experimental exercise, different contexts or settings were simulated and the exercise, once again found support for the three factors as significant antecedents to privacy concern. The only deviation from these otherwise consistent findings was that extroversion was not a significant determinant of privacy concerns in a healthcare setting.

Personality, as measured by the Big Five and based on at least some of its dimensions, was found to have a strong relation to privacy. Studies have consistently measured how different dimensions of an individual’s personality may predict privacy measures. However, analyzing the relationship between each personality trait and each of
the dimensions of privacy concern, has not been conducted in the extant literature. This represents an opportunity to examine this relationship at a more granular level which may be able to explain the relationship in further detail.

2.4.5.1.3 Other Internal Antecedents to Privacy

Other noteworthy internal antecedents to privacy concerns studied in the literature include affect, age, health status and trust. (Bansal et al., 2010; Belanger et al., 2002; J. Frost et al., 2014; Kordzadeh & Warren, 2017; Krasnova et al., 2010; Miltgen & Peyrat-guillard, 2014; Sato & Costa-i-Font, 2013; Wakefield, 2013; Yu et al., 2015). Finally, it should be noted that trust, last in the previous list, has also been studied as an antecedent to perceived privacy risk (Malhotra et al., 2004), with increased trust reducing perceived privacy risk. Trust is one of the few antecedents that reduces perceived privacy risk and privacy concerns, and thus provides an opportunity for further analysis of this relationship.

2.4.5.2 External Antecedents to Privacy

2.4.5.2.1 Country Culture

Country culture is an external, context characteristic antecedent utilized in two different studies in the present review. Based on the Hofstede, (1980) taxonomy of five cultural dimensions, and focusing on the collectivism vs. individualism dimension, Miltgen & Peyrat-guillard, (2014) showed that people from different countries in Europe differ in their privacy concerns. Those from collectivist countries express more trust and are less reluctant to disclose information than are those from individualistic countries. The study also confirms previous findings (Palfrey & Gasser, 2008) asserting that
younger individuals show significantly less privacy concerns than adults. Lowry et al., (2011), while using Hofstede, (1980) taxonomy, chose to measure four dimensions: masculinity, uncertainty avoidance, power distance, and individualism vs. collectivism. This survey-based study compared a respondent sample of undergraduate students in China versus United States and concluded that all but masculinity were significant predictors of privacy concerns. Finally, Posey et al., (2010), measured individualism and collectivism as predictors of self-disclosure. This study considered groups from the UK and France and found collectivism to be moderately significant in its relationship to self-disclosure, while individualism was not significant. The Posey et al., (2010) study is the only one set in an online community context and is therefore an important informant to the purpose of current literature review study. The studies in this section offer mixed perspectives with regards to the role of country culture as an antecedent to forms of privacy. These mixed results suggest the need for further research on the relationship between culture and forms of privacy and lends itself to clear opportunities for research extension.

2.4.5.2.2 Information Sensitivity

In the context of healthcare, there is one antecedent that, although apparently important, seems to be largely unexplored in relationship to privacy: information sensitivity. Bansal et al., (2010) demonstrates a significant effect of information sensitivity on privacy concern in a healthcare setting. Kehr et al., (2015) found mixed results for the effect of information sensitivity in a mobile application as a significant predictor of perceived privacy risk. Information sensitivity warrants additional examination, particularly in the context of healthcare.
2.4.6 Outcomes to Privacy-Related Constructs in the Literature

Given the previous discussion of all measured antecedents to privacy-related constructs, this section summarizes all of the outcome variables which have been documented as being influenced by privacy-related constructs. Twenty-one different outcomes to privacy-related constructs were identified in the literature. The outcomes are organized again based on the Theory of Reasoned Action (TRA), and are thus presented as beliefs/attitudes, intentions, and behaviors. Table 2.4 presents a list of all the outcomes with the reference number, indicating which article they are found in. Additionally, and congruently with the previous analyses, the constructs might not share the exact same name but were grouped together nevertheless for having highly similar operationalizations. For example, in the context of their study, Andrews et al (2014) refers to the intention to use a personally controlled electronic health record simply as “intention”. Therefore, the intention in their study has been classified in the present analysis as behavioral intention.

Table 2.4 - Outcomes in the privacy literature.

<table>
<thead>
<tr>
<th>Beliefs/Attitudes</th>
<th>Intentions</th>
<th>Behaviors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trust (1, 2, 6, 9, 27)</td>
<td>Intention to disclose information</td>
<td>Self disclosure</td>
</tr>
<tr>
<td></td>
<td>(1, 9, 11, 18, 26, 30, 32, 39, 44, 46, 47)</td>
<td>(7, 19, 35, 38, 43, 45, 48)</td>
</tr>
<tr>
<td>Attitude towards technology (12)</td>
<td>Intention to adopt</td>
<td>Privacy protective behaviors</td>
</tr>
<tr>
<td></td>
<td>(4, 35, 37, 42, 52, 53)</td>
<td>(15, 16, 29, 49)</td>
</tr>
<tr>
<td>Regulatory preferences (20)</td>
<td>Behavioral intention</td>
<td>Subsequent behaviors</td>
</tr>
<tr>
<td></td>
<td>(3, 22, 23, 25, 27, 33)</td>
<td>(10)</td>
</tr>
<tr>
<td>Tourism satisfaction (24)</td>
<td>Purchase intentions</td>
<td>Purchase decision</td>
</tr>
<tr>
<td></td>
<td>(44)</td>
<td>(5)</td>
</tr>
<tr>
<td>Subsequent beliefs (10)</td>
<td>Willingness to delegate profile</td>
<td>Reciprocity</td>
</tr>
<tr>
<td></td>
<td>to apps (17)</td>
<td>(7)</td>
</tr>
<tr>
<td></td>
<td>Continuance intention (21)</td>
<td>Social network use for medical information (14)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Technology usage (51)</td>
</tr>
</tbody>
</table>
2.4.6.1 Outcomes as Beliefs/Attitudes

The following sections present the reader with a synthesis of the most commonly used outcomes of privacy-related constructs in the literature that can be understood as beliefs or attitudes.

2.4.6.1.1 Trust

A commonly used belief/attitude outcome in the literature (by count of times used) is trust. Trust has been studied as a mediator between privacy concerns and intention to disclose information (Xu et al., 2009) and has been studied as an antecedent to privacy (Belanger et al., 2002). As discussed previously, trust has been studied closely for its relationship and most notably, its influence on privacy. However, as shown here, it has also been studied as a privacy related outcome. Bansal et al., (2010) has shown that trust decreases due to negative prior privacy experiences and its direct impact on perceived privacy risks. In a demographic-level analysis, trust has been shown to decrease more dramatically for females than for males because of privacy concerns (Midha, 2012). Bansal et al., (2015) also demonstrated that privacy concerns influence trust and trust subsequently impacts intention. Finally, Malhotra et al., (2004) proved the same relationship while testing the role of risk beliefs as a mediator between trust and behavioral intention. All these studies, however, explain the opposite relationship to those which use trust as an antecedent to privacy. Krasnova et al., (2010), for example, shows trust as a preceding measure to perceived privacy risks and them (perceived privacy risks) alternatively having a negative relationship to self-disclosure. As evidenced during the analysis of antecedents, the directionality paradigm holds true from the outcome perspective as well.
Beliefs and attitudes determine intentions. Intentions are characterized by a change in the likelihood of engaging in a specific action or behavior as a result of a process (usage, exposure, interaction, etc.). A purchase intention, for instance, is augmented when an individual feels more safe, secure, or trustful about a vendor, for instance, (Belanger et al., 2002) and therefore is more willing or likely to execute a purchase from them.

2.4.6.2 Outcomes as Intentions

This section reviews those intentions that are outcomes of privacy-related constructs. Intentions are plans toward an action or behavior but not the actual behavior (Floyd et al., 2000). In survey research, intentions are much more often used for surveys are not used to measure actual behaviors.

2.4.6.2.1 Intention to Disclose Information

Intention to disclose information is the single most used outcome in the extant privacy literature. Evidently, in information systems, information disclosure is an important outcome of privacy and across studies these constructs seem to have a predictable negative relationship. Intention to disclose information is a summary evaluation regarding the likelihood to voluntarily offer one own’s personal information. Although from a definition perspective there is not much variability on this concept, from an application standpoint, the context of disclosure is widely different (Sheng et al., 2008). In an e-commerce setting, for example, disclosure of sensitive information can have financial undesirable results (risks) such as fraud (Bansal et al., 2016). In a healthcare context, the sensitivity of the information is more related to a sense of
embarrassment or discrimination avoidance (Kordzadeh & Warren, 2017). However, in other settings such as social media or general information seeking, the exchanged information may not share the sensitivity of the former examples. As such, the context analysis of intentions to disclose is consistently important.

2.4.6.2.2 Intention to adopt

Intention to adopt is the second-most used attitudinal construct found in the literature. Adoption intention relates to the likelihood of utilizing a service, application or other technological artifact. When the utilization of such technologies involves the exchange of sensitive information, the perceived privacy risks are increased and the likelihood of usage, or intention to adopt are reduced (Crossler & Posey, 2017; Lowry et al., 2011). The studies consistently found a negative significant relationship between privacy-related measures such as privacy concerns or perceived privacy risks and the intention to adopt certain technology. The following examples illustrate the context gamut in which intention to adopt has been analyzed:

- Intention to adopt mobile applications (Gu et al., 2017)
- Privacy management tools, identity ecosystem (Crossler & Posey, 2017)
- Personalization services in e-commerce (Sheng et al., 2008)
- Social computing technologies i.e. Social media (Lowry et al., 2011)
- Electronic Health Records (Angst & Agarwal, 2009)

The variability of intention to adopt has been demonstrated to depend on the context (Sheng et al., 2008) and information sensitivity is different from setting to setting.
However, this sample of articles did not analyze sensitivity of the information nearly as commonly as a potential driver of adoption as it looked at other measures.

2.4.6.3 Outcomes as Behaviors

Behaviors measure actions taken by an individual. This category contains a well-represented number of outcomes found in the literature. Among them, self-disclosure, privacy protective behaviors, purchase decisions, reciprocity, and usage of technologies are found. Two of the most common outcomes are discussed in the following paragraphs

2.4.6.3.1 Self-Disclosure

Self-disclosure is defined as “the amount of personal information that an individual shares with another” (Wakefield, 2013; pp. 159). It is consistently shown to be negatively correlated to privacy concerns. This relationship is illustrated in the social network setting where the amount of information individuals share about themselves depends on the different levels of privacy concerns they display (Kehr et al., 2015). Self-disclosure is found in seven different articles in the literature as a behavior-type of privacy related outcome. For the purposes of this study, self-disclosure is arguably one of the most relevant constructs of the literature as it directly pertains to the use of online health communities. While closely related to intention to disclose, the difference between intention to disclose and self-disclosure lies on how the construct has been operationalized in a specific study: while intention measures the attitude regarding disclosing, self-disclosure measures the actual action (behavior) of providing information. Due to this, self-disclosure lends itself more naturally to be adopted for experiment-type of studies. As mentioned before, self-disclosure is the individual’s action
of sharing his/her personal information. In an online health community, the wealth of information of an OHC is made up of all the information surrendered by its users and is therefore at the heart of the analysis in this review.

Posey et al., (2010) propose that reciprocity is one of the drivers for self-disclosure. In their study, reciprocity is defined as a special form of social influence that represents the key benefit influencing self-disclosure. Also known as the dyadic effect, reciprocity is a quid-pro-quo mechanism that is self-generating. This means that the more information people share in a setting, the more others are willing to share as a result. Perhaps this is the most salient observation of the analysis of reciprocity and self-disclosure.

2.4.6.3.2 Privacy Protective Behaviors

Privacy protective behaviors represent a wide spectrum of activities users may engage with in order to protect their personal privacy. Set in an online social networks context, James et al., (2017) investigates the actual usage of privacy controls within a social networking site. Referred to as privacy controls, the authors find that users in fact opt for the usage of this type of tools to address potential privacy concerns. In the OHC setting, it would hold, that providing privacy controls to users can help alleviate privacy concerns and improve the amount of contributions from members of the community.

2.5 Nomological Model: Classified Antecedents to Types of Outcomes

In the preceding analysis of the literature, the antecedents to privacy-related constructs have been categorized into four distinct groups (internal/external antecedents), and the outcomes into three groups using TRA as framework. In order to create a visual
mapping of how the relationships between antecedents and outcomes are represented in the sample of articles across this literature review, the following nomological model (Figure 2) has been created. The utility of this visualization stems from its capacity to summarize the relationships among the different types of antecedents and outcomes to privacy that exist in the literature. From it, potential opportunities for future research are observed.

Based on Figure 2.1, it is evident that internal antecedents have received attention in privacy research with 10 individual differences and 15 perceptions/beliefs studied as determinants of privacy concerns or risk. On the other hand, we can also see that external antecedents have received consideration, but not the same as internal antecedents, with 8 artifact characteristics and 7 context characteristics examined as determinants of privacy concerns or risks. In the context of OHCs, this represents a clear opportunity for continued research. Not only the web context lends itself naturally for experimental

Figure 2.1 - Integrated Nomological Map of Privacy Studies.
studies, but external antecedents such as artifact characteristics are easier to manipulate/alter to achieve a specific purpose. From an outcome perspective, 25 studies have examined how privacy concerns or privacy risks have influenced intentions such as willingness to disclose or in intentions to adopt. Further, 15 studies have examined how privacy concerns and perceived risk affect behavior or actual disclosure of personal information. Finally, 9 studies have analyzed how privacy concerns or risk may influence beliefs and attitudes. Opportunity exists for researchers to measure artifact and context characteristics as antecedents to privacy risk and concern. This is congruent with the previous observation that more research should measure information sensitivity (a context characteristic) for its impact on different outcomes.

2.6 Future Research, Limitations and Conclusion

After the initial selection of articles for this literature review, there was an evident low number of publications representing the medical technology field. While the initial results showed promise, there were few articles with empirical analysis at the individual level (Andrews et al., 2014; J. H. Frost & Massaglia, 2008; Sato & Costa-i-Font, 2013). This constitutes the first observation of this literature review: An ample opportunity for IS researchers exists in medical journals for carrying out empirical research on privacy. Given its presence and consistent findings, the construct of prior privacy invasions is an effective correlate to privacy and privacy concerns. Such is the agreement among studies that perhaps researchers can focus their efforts on extensions or non-existent treatments of the construct. Similarly, when a correlate of privacy concerns is desirable for statistical purposes, this could be a potential measure to utilize.
Personality traits (Big Five; NEO) have been studied as antecedents to privacy concerns. However, scales measuring personality traits are lengthy and have exhibited lower reliability, especially among its short scale versions (Donnellan et al., 2006). Further exploration of this potential relationships, as well as the evaluation of other personality measures might prove pertinent in the study of online privacy.

Privacy assurances seem to have largely achieved consensus as being significant influencers on the sense of privacy an individual can derive from the use of an artifact. Therefore, it is essential to emphasize these attributes of the technology tools in their effect over individual’s privacy attitudes and behaviors. As a concept, however, they have not been defined consistently in the field (Lowry et al., 2011; Xu et al., 2011a), and have only been explored in a few studies. While some authors suggest use of any characteristic of the artifact, others are very specific about which types of elements can be interpreted as assurances. The Federal Trade Commission’s guidelines (Federal Trade Commission, 2000) referenced in this study provide a promising template that has already been empirically measured as strong predictors of privacy (Liu et al., 2005). Perhaps, these guidelines can aid the development of an academic focused construct measuring privacy assurances.

Country culture, as an antecedent to privacy has been only partially, and selectively studied. Hofstede’s model is not the only measure of culture identified in the literature, and only one or two of its dimensions have been consistently used. The extant literature concerning this relationship offers clear opportunities for research extensions. Other considerations such as country-specific legal protections or financial considerations pertinent to different markets or economies (although arguably not strictly cultural
dimensions) can be explored in future studies. Further, the uncertainty avoidance index (another of Hofstede’s cultural dimensions) remains unexplored as a predictor of privacy or any of its related constructs. In the online setting, with only one study to speak for, given its world-wide applicability, this seems a very appropriate and potentially impactful exploration that may inform theory and practice alike.

Trust and privacy risks have been successfully validated as antecedents to each other (Bansal et al., 2010; Malhotra et al., 2004). This might represent an opportunity for researchers to explore the theoretical relationship of these two constructs. A potential theoretical contribution may be waiting to be identified in the directionality relationship of these constructs.

One of the most prevalent constructs in privacy studies in the IS field is the concept of privacy concerns. However, it is important to consider that it was not designed as a tool to measure privacy in an online setting. Although other conceptualizations have been proposed, none is even closely as popular as privacy concerns. Malhotra et al. (2004) proposed the Internet Users Information Privacy Concern (IUIPC) model. However, this operationalization of privacy concerns has not been widely adopted in subsequent research. This could represent an opportunity for researchers to revalidate their past findings utilizing more setting-specific measures.

A key concept in the OHC studies of privacy is that of self-disclosure. Although a few papers describe it as an outcome of an attitude motivated process, only one (Posey et al., 2010) described it as a function or outcome of possible social benefits such as reciprocity. This is a major opportunity of research since the tradition has focused on efforts minimizing the risks and concerns to promote disclosure. This is only a deficit-
based approach. Instead, the positive analysis of this phenomena (that is, as it relates to potential benefits) is limited at best.

Individuals with a given level of privacy concerns are found to utilize tools within the websites that give them more control of their privacy. In OHCs, these tools or controls can prove to be a mitigating form to alleviate privacy concerns among patients and users in general. Considering the importance which the concept of control has had in relationship with privacy (Belanger & Crossler, 2011), further investigation into the role of control is granted. Furthermore, and considering the importance of this conceptual gap, new definitions and operationalizations of control should be studied in its relationship with privacy.

2.7 Limitations

As with any research project, the present literature review has its own limitations due to the scope, chosen methodology and even its own findings have revealed potential ways in which this work could be advanced. First and foremost, the selection of a specific group of journals as the potential sources for qualifying articles could represent a weakness and an opportunity for future research. Including more journals as well as dissertations and conference proceedings may yield a richer body of literature.

Limiting the selection of articles to the individual level clearly offers some advantages such as being able to focus on the personal mechanisms driving privacy and privacy-related concepts. However, as discussed in previous sections, a large portion of the privacy studies, especially in the healthcare technology journals, was removed from the analysis in the present study. Health technology journals often consider the
organizational level of analysis as basis for their studies. Although organizational level treatments tend to deal more with the information security, some studies could potentially contribute to the development of the topic from a theoretical perspective. Finally, due to the larger number of general IS articles (compared to healthcare), as well as the research not focusing strictly on the online setting (in the health tech journals), the observations offered in this research might not be as context-specific as they would ideally be.

2.8 Conclusion

Privacy in online health communities represents an untapped source of research opportunities. As illustrated by the present study, not only the amount of literature in the topic is limited, but there are general aspects of privacy that are yet to be explored in this specific setting. A primordial example is the role that control plays in the generation of privacy concerns. Although the concept of control is central to privacy, the IS field is still to capitalize on the analysis of information control as a remedy for privacy concerns. The reduced utilization of different theoretical conceptualizations of control in different settings or contexts is one specific example of how this literature gap may be addressed in the future.

From observing and analyzing the relationships among types of privacy-related constructs in the privacy nomological network, other gaps are identified. It is apparent that relationships between external characteristics of the artifact have been only sparingly studied as predictors of intentions or behaviors. Research which follows this construct relationship recipe will only add to the body of literature.
Privacy is a very relevant topic of our day in information systems. This literature review provides a detailed description of the research of privacy at the individual level. Some important opportunities for future research efforts have been identified and a specific application for the context of online health communities has been proposed. As healthcare technologies continue to push the boundaries of traditional medical treatment, the IS field must actively try to anticipate challenges and propose alternatives that result in the overall protection and services of the users of online health communities. Finally, an overall recommendation is for privacy research to use tools (measures and scales) that have been designed with web communications in mind. As we witness advances in communication technologies, it is due diligence for the field of IS to continuously redesign and innovate the tools used to generate new knowledge on information privacy.
CHAPTER 3

PRIVACY ASSURANCES, CONTROL, AND INFORMATION SENSITIVITY ON THE INTENTION TO DISCLOSE INFORMATION: AN EXPERIMENTAL STUDY

3.1 Introduction

Personal information collection is still at the heart of business-to-consumer e-commerce. Companies depend in great measure on the amount of information they are able to collect from their customers to design products and services that are of interest and utility for their customer-base (Hui et al., 2007). In contrast to this interest, customers face important safety concerns when asked to provide personal information. This is especially true at the time of transacting with a company with which they haven’t dealt before (Y. Li, 2014). The loss and exposure of personal information through online hacking episodes, software security flaws, internal leaks, data misuse, etc., are part of everyday news, yet companies seem to possess limited ability to protect their customers’ information (Martin et al., 2017). These stories have a powerful impact on users’ privacy concerns and their willingness to disclose personal information. Reconciling these opposed but congruent interests is a matter of continuous debate in information systems (IS) research.

One way to mitigate privacy concerns and encourage sharing of personal information is through the use of IT-related privacy assurances. These IT artifacts are “…mechanisms that directly or indirectly provide customers with assurances and guarantees that their private information will be protected and kept private by the
website” (Bansal et al., 2015; pp. 625). Assurances are attributes of the IT artifact, such as icons, badges or text (Lansing et al., 2019), that hold promise to assuage individuals’ concerns stemming from sharing their information on vendors’ sites.

Control, defined as “the interest an individual has in controlling, or at least significantly influencing, the handling of data about themselves…” (Belanger & Crossler, 2011), is also a powerful influence on an individual’s decision to disclose information. Individuals who have complete control over what will be done and who will have access to their information, may intuitively derive an enhanced intention to disclose said information (D. L. Stone, 1986). While IS research has examined control as an important dimension of privacy concerns, control has received less attention as an antecedent to important privacy-related outcomes and behaviors.

Information sensitivity, when information is more or less personal to the individual, necessarily influences privacy-related outcomes. This construct explains how individuals respond differently to requests for information, even when the same privacy assurances and control are provided. When the information to be given to companies is seen by individuals as more sensitive, they will feel more protective of it (Rohm & Milne, 2004). Companies can lean on two particular aspects to compensate for this sensitivity: first, companies may let users know the business’ intentions with regards to the storage and sharing of information and inform users how their information will be safeguarded. On the other hand, businesses can opt to involve the users in the management of information, giving individuals the ability to determine what can and cannot be done with the information they provide. These two strategies correspond to privacy assurances and privacy control. Put in a different way, while information
sensitivity tends to make users/customers more protective of their information (and therefore, less willing to provide information), privacy assurances can appease this fear by showing the intentions and capabilities of the company (Hui et al., 2007). At the same time, companies can provide users a degree of control over the information, so they feel more empowered by the usage of this information and, therefore, more willing to provide information (Neves & Caetano, 2006). Privacy assurances and personal control over sensitive information are thus important considerations for consumers as they weigh the benefits and costs of sharing their personal information online. While IS research has examined some antecedents and outcomes of online privacy concerns (Bansal et al., 2010; Junglas et al., 2008; Y. Li, 2014; Miltgen & Peyrat-guillard, 2014), limited research has examined these antecedents as a means to encourage users to disclose personal information online.

Alongside the previously discussed constructs of privacy assurances, control and information sensitivity, this study relies on the privacy calculus model (Dinev & Hart, 2006) as the theoretical background. Privacy calculus is a research model incorporating the most common and important constructs in the privacy literature. These include privacy concerns, perceived risk, trust and the intention to disclose information. This theoretical model has enjoyed a prominent space in the information systems literature and is often described as an individual-level analysis of the positive and negative aspects of the transaction at hand and how it informs the person’s intention to disclose information.

An experimental design in the context of online web services is used to examine privacy assurances, control, and information sensitivity as antecedents to constructs in the privacy calculus model. In the following sections, the theoretical background of the
privacy calculus model and the definitions and sources of the study’s major constructs are first described. Next the research model and hypotheses are presented. The study’s experimental design and analysis is reported, followed by discussion and conclusion.

3.2 Theoretical Background

In this section, a review of the IS literature on privacy and the privacy calculus model is provided. Privacy assurances are reviewed as an IT artifact that can promote trust towards the online vendor and encourage sharing of information. Information sensitivity and personal control are also reviewed as highly relevant attributes of any online privacy context.

3.2.1 Online Privacy and the Privacy Calculus

The privacy calculus (Dinev & Hart, 2006), was first published with the intention of capturing relevant and literature-proven constructs to address two different sources of influence in the privacy phenomena: positive and negative, as shown in Figure 3.1. Positive forces aiding the information disclosure is are personal internet interest (PII) and the trust an individual develops for the vendor/company. PII is an individual trait-like degree of motivation for the online transaction which can have an amplifying effect (and is described as a direct antecedent to) the intention to disclose information (ITD). Trust on the other hand is the degree to which an individual is willing take on a certain level of risk and is typically described in the literature as a pre-condition to the intention to disclose. Trust is proposed in the model to mediate the effect of perceived risk onto the intention to disclose information.
The second source of influence in the privacy calculus can be seen as a negative source in the privacy phenomena since it results in a diminished intention to disclose information. The two constructs in this group are the *privacy concerns* and the *perceived risk*. Privacy concerns is perhaps the single most used construct in privacy studies in IS and it captures different dimensions of individual concern related to privacy (J. Smith et al., 1996). In the privacy calculus model, privacy concerns are modeled as mediating the effect of risk on the intention to disclose information. Privacy concerns have been demonstrated to be a major barrier preventing participation from individuals in the online setting (Y. Li, 2012). The second construct, perceived risk, is the evaluative measure of the individual related to the perceived degree of potential associated loss related to the exchange of information. (Jarvenpaa & Tractinsky, 1999). Risk plays an important role in the model since it is modeled as being a direct antecedent to intention to disclose information, but also two indirect effects on intention to disclose information: One, mediated by trust, and one mediated by privacy concerns. Perceived risk is also found in the literature to have the potential to prevent individuals’ participation online (Andrews et al., 2014; Bansal et al., 2010; Kehr et al., 2015).
The full model was coined the “privacy calculus” which is commonly explained as the result of weighing the potential benefits versus the potential downsides of disclosing information online. Such description stems precisely from the fact that two constructs present a favorable influence while two others represent the negative aspects which can result from this disclosure of information. The privacy calculus research model is based on the Theory of Reasoned Action (Ajzen & Fishbein, 1975) where behavioral intentions are the result of individual attitudes and subjective norms. In it, the behavioral intention is represented by the intention to disclose information whereas the attitudes and subjective norms are represented by privacy concerns, risk and trust.

3.2.2 Privacy Assurances

Privacy Assurances have received special attention in the literature. Bansal et al., (2015) defines privacy assurances as “mechanisms that directly or indirectly provide customers with assurances and guarantees that their private information will be protected and kept private by the website.” (pp. 625) Upon closer inspection, however, the
conceptualization and operationalization of assurances has varied widely within the literature. Some authors have operationalized assurances with statements or seals of privacy guarantee in websites (Lowry et al., 2012). Others have conceptualized it as the perceived effectiveness of privacy policies or the effect of regulation (Xu et al., 2011a), while others have adopted other definitions as well. Additionally, not all research evidence tells a consistent story. Some studies have found conflicting results while evaluating the role of privacy assurances (Hui et al., 2007). For the context of our study, privacy assurances are defined as seals and statements that indicate a degree of care in the part of the company for the proper management of users’ information and privacy.

3.2.3 Control & Privacy

“Information privacy refers to the concept of controlling how one’s personal information is acquired and used…” (Pavlou, 2011; pp. 977). “…many researchers have suggested that privacy is one’s ability to control information about oneself…” (Belanger & Crossler, 2011; pp. 1018) These two quotes come from important literature reviews on privacy in information systems, use the concept of control as a central component of the definition of privacy. However, the large majority of studies investigating the phenomena in Information Systems (IS) have not incorporated an empirical measure of control in their research. The widely adopted privacy concerns (J. Smith et al., 1996) is a four-dimension construct that doesn’t measure the degree of control an individual has over his/her information.

Two important considerations have been taken into account for the inclusion of the control construct in the current study: First, as mentioned above, control is an important, yet neglected, component of the concept of privacy and, second, the privacy
calculus, which is previously described in this manuscript is based on the theory of reasoned action (TRA) (Ajzen & Fishbein, 1975), was in fact later used as the basis for the theory of planned behavior (TPB) (Ajzen, 1991). In this theoretical extension, the author added the *perceived control* construct as a third antecedent to the behavioral intention. One of the goals of the present investigation is to understand how important this notion of *control* can be in the privacy phenomena. For the purposes of our study, control is defined as the degree of influence, an individual has over the collection, use, and distribution of their information.

### 3.2.4 Information sensitivity

One apparent aspect of privacy is its context and previous studies have looked at the context or information sensitivity as an antecedent to some aspect of the privacy phenomena (Bansal et al., 2010; Malhotra et al., 2004). For the latter study, interviews with participants utilized a scenario-based questionnaire where they described two scenarios, one with personal shopping preferences, while the other scenario involved personal financial information. For the Bansal et al., (2010) study, the authors asked all participants to rate the perception of sensitivity of health information to investigate the role of sensitivity as an individual trait. The widely accepted notion is that there are some specific categories of information that tend to be considered more personal or private than others (Sheehan & Hoy, 2000). The literature has specified the need for “Future research on information privacy tools and techniques should likewise be more contextually sensitive.” (Belanger & Crossler, 2011). This analysis can be particularly useful if a new combination of other constructs can be included as part of the same study.
An experimental setting where the sensitivity can be manipulated to evidence its impact in the outcome variables can provide a rich insight on the nature of the construct.

3.3 Research Model and Hypotheses

The focus of this research is to better understand the effectiveness of privacy assurances, as well as the effects of information sensitivity and personal control, on the outcomes considered in the privacy calculus model: context-specific privacy concerns, risk and trust, which serve as mediator variables to the intention to disclose information. Age, gender, prior privacy violations and the agreeableness dimension from the Big 5 Personality inventory (Donnellan et al., 2006) are treated as control variables for either having been consistently shown to be significant antecedents of privacy. As the chosen theoretical foundation, the privacy calculus (Dinev & Hart, 2006) is a central component of the research model of this study and as such is kept in its original form within the overall design of the present research model. The experimental portion of the study is adopted as a set of antecedents to different parts of the privacy calculus model as seen in
In figure 3.2 above, privacy assurance, control, and information sensitivity, serve as antecedents or inputs to the privacy calculus model. These novel aspects of the model form H1 through H6. The relationships among the constructs in the privacy calculus model form from H7-H11. Given the limited empirical studies that have tested this comprehensive model, these relationships are also presented as hypotheses, and contribute to the privacy literature.

Control as a construct is of great importance in the privacy literature. In fact, a 2011 review of privacy research (Belanger & Crossler, 2011) defined information privacy as “the interest an individual has in controlling, or at least significantly influencing, the handling of data about themselves.” Control has also been included in some
conceptualizations of privacy concerns as a first order dimension of the second order privacy concerns construct (Malhotra et al., 2004), and operationalized with a scale. This conceptual and empirical work acknowledges the potential importance of the control-privacy relationship, while also leaving a gap in our understanding, as the most commonly used conceptualization of privacy concerns does not include control (J. Smith et al., 1996). And, the study of control as a first order dimension of privacy concerns does not support examination of control as a determinant of privacy and other privacy-related constructs. Culnan et al., (1999) explained that “…individuals are less likely to perceive information collection procedures as privacy-invasive when […] they perceive that they have the ability to control future use of the information…” (pp. 106). Control as a determinant of privacy concerns holds promise but has received limited attention (e.g., Xu et al., 2012). Therefore, the present research model proposes:

H1: Higher levels of personal control over data decrease privacy concerns.

As a dimension of privacy concerns, or as a potential determinant of privacy concerns, control should also influence perceived risk. While this relationship has received limited attention in the literature (Zhang et al., 2018), the relationship between perceived risk and privacy concerns is well-supported. (Xu et al., 2011b; Dinev et al., 2013)When Malhotra et al., (2004), proposed the Internet Users Information Privacy Concerns as a new scale for measuring privacy concerns, they showed the impact of this new proposed measure on the individual risk beliefs. The privacy calculus model (Dinev & Hart, 2006) also depicts a relationship between perceived risk and privacy concerns. Though the literature has considered control and perceived risk as important constructs in the study of privacy, no studies have identified control as an antecedent to risk formation,
likely because empirical work has just started to consider control as a separate construct. Just as greater control over one’s personal information could decrease privacy concerns, it stands to reason that control could reduce the perceived risk in disclosing information, if a user perceives that s/he can control what information is shared and how that sharing occurs. Thus, this study hypothesizes:

H2: Higher levels of personal control over data decrease perceived risk.

Wang & Herrando, (2019) show the significant impact regulation has on trust. The granting of control over personal information to a user also has the potential to influence trust formation between a user and a company. Research has shown that trust formation towards an e-commerce site can be influenced by a company’s regulatory compliance and actions taken as part of that compliance (Wang & Herrando, 2019). Similarly, research suggests that an opt-in strategy for sharing personal information builds trust (Urban et al., 2009). When an individual depends on a third party to achieve something, a degree of trust, relative to the accepted risk is a pre-requisite to the relationship (Whitener et al., 1998). If a company gives the individual a degree of control over the management of their personal information, this act of control-giving may enhance the trust that the individual will feel for the service provider. Therefore, it is hypothesized that:

H3. Higher levels of personal control over data increase trust toward the company.

The literature has demonstrated the role of information sensitivity in face-to-face contexts of commerce and marketing where individuals clearly adopt a more protective
stance towards their information when this information content is sensitive or private, such as finances (Phelps et al., 2000). The degree of sensitivity conceptualized as the innate private nature of the information (Milne, 1997; Sheehan & Hoy, 2000) should likewise influence privacy concerns. While limited research has considered the influence of information sensitivity (e.g., Malhotra et al. 2004), even less research has considered a formal relationship between information sensitivity and context-specific privacy concerns (Bansal et al., 2010). Consumers appear generally more concerned about the collection of medical records, social security numbers and financial information (Sheehan & Hoy, 2000) and prior studies have shown increased sensitivity for health information (Bansal et al., 2010). Therefore, this study hypothesizes:

H4. Higher levels of information sensitivity increase privacy concerns.

As described above, the degree of information sensitivity has received limited attention in the privacy literature. In Malhotra et al., (2004), a scenario-based study was conducted comparing participants’ shopping preferences versus the participants’ financial information on privacy-related outcomes. Support was found for the financial setting being more ‘sensitive’ and having a positive, increasing effect on perceived risk. Surprisingly, this relationship is not widely studied and has not been considered in the context of healthcare information. Bansal et al., (2010) does examine information sensitivity and perceived risk, however, a relationship between these constructs is not proposed and sensitivity is measured as an individual-level pre-existing trait, and not in relation to a specific information sharing context. Angst & Agarwal, (2009) also observe and emphasize the need for further investigation of the issue of information sensitivity, as
sensitivity is associated with the value of the information, and thus more valuable information would represent a larger risk. Thus, this study hypothesizes that:

H5. Higher levels of information sensitivity increase perceived risk.

Privacy assurances provide an IT-enabled approach to reducing risk and increasing trust in an information sharing context. Belanger et al., (2002) argue that a first step in establishing consumer trust is providing assurances that the consumers’ personal information will be protected. Furthermore, an empirical study showed evidence for the positive effect of assurances in the formation of trust among customers (McKnight & Kacmar, 2004). Although different authors have operationalized assurances in different ways (Lowry et al., 2012; Xu et al., 2011a), the overall consensus points to the fact that website or other IT technology attributes that explicitly reassure users about the treatment of their personal information, lead to higher levels of trust among individuals. Privacy assurances can be any elements of the artifact that communicate a degree of security. Lowry et al., (2014) demonstrated how specific components of a website can have an impact on user trust. In addition to sharing information about how a company will safeguard personal information, privacy assurances can transmit a degree of professionalism, care and other positive vendor characteristics that will aid in trust formation. It is, therefore, hypothesized:

H6. High levels of privacy assurances increase trust towards the site.

Perceived risk and privacy concerns are related constructs that have been widely studied in the IS literature. In an online context, these privacy concerns are related to all aspects of the transmission, storage and subsequent use of the information surrendered by
internet users. An individual’s heightened perception of general risks has been shown to have a negative impact on privacy concerns. Most notable is the relationship depicted in the privacy calculus model (Dinev & Hart, 2006). Other examples in the literature have supported a relationship between perceived risk and privacy concerns (Hong & Thong, 2013; Jarvenpaa & Tractinsky, 1999). James et al., (2017), and Malhotra et al. (2004). While there are different opinions on the direction of the relationship between these constructs, this research adopts the directional relationship proposed by the privacy calculus model (Dinev & Hart, 2006), with perceived risk influencing privacy concerns. Thus, this study hypothesizes that:

H7. The perceived risk of sharing data with an online company will be positively related to an individual’s privacy concerns.

Likewise, the IS privacy literature has previously examined the relationship between risk and trust, albeit in different privacy contexts. Some studies have depicted the relationship with trust being an antecedent of risk (Jarvenpaa & Tractinsky, 1999; Malhotra et al., 2004) while others have proposed the opposite causal relationship (Dinev & Hart, 2006). An intent analysis of the relationship between these two constructs would suggest that risk is best modeled as an antecedent to trust because it is a quick evaluation of the situation at hand. Conversely, trust is a more elaborate process that requires a higher degree of cognitive involvement and analysis from the perspective of the users (McKnight & Kacmar, 2004). Cross-discipline literature on this topic is abundant (Holmes, 1991; Solhaug & Stølen, 2012; Weber et al., 2004). In line with the proposed directional relationship of the privacy calculus, this study proposes:
H8. Perceived risk will negatively impact the trust an individual has for an online vendor.

Privacy concerns and the requirement to provide information online have been reported as significant barriers that discourage individuals from transacting online (Miltgen & Peyrat-guillard, 2014), and are documented in the IS privacy literature (e.g., Zhang et al., 2018). When transacting online, if a user’s privacy concerns are high, they will be less likely to share information and may avoid transacting online, to avoid exposure to such potential negative effects (Dinev & Hart, 2006). As such, this study hypothesizes:

H9. Privacy concerns are negatively related to an individual's intention to disclose information.

Just like privacy concerns are expected to have a negative impact on the intention to disclose information, perceived risks will be expected to act in a similar fashion. When individuals have a reduced interpretation of risk, they are more likely to share information. This relationship has been demonstrated in the extant literature (Awad & Krishnan, 2006; Malhotra et al., 2004; Dinev & Hart, 2006). Individuals perceiving an elevated degree of risk are more likely to engage in protective behavior (James et al., 2017; Miltgen & Smith, 2015). Arguably, concealing one’s personal information could be considered such type of privacy-protective behavior reinforcing the notion that in the presence of risky situations, individuals will avoid providing information. Thus, this study hypothesizes that:

H10. Perceived risk is negatively related to intention to provide information.
In IS research, trust has played an important role in understanding behavioral intentions, with behaviors including IS adoption (Karahanna et al., 2003) and online purchases (McKnight et al., 1998). Social cognitive theory supports the relationship between trust and relationship behavior, since the degree of trust is a positive general influence on the relationship between two individuals. Behavioral intentions and actual behavior around disclosure of information online are similarly influenced by trust, as documented in the privacy calculus model (Dinev & Hart 2006). This relationship has also been supported in research employing different conceptual models (e.g., Bansal et al., 2015; Kehr et al., 2015; Weber et al., 2004). Therefore, I hypothesize:

H11. Trust is positively related to an individual’s intention to disclose information.

Personal Internet Interest (PII) is a construct that expresses an individual’s intrinsic motivation to accomplish something online (Dinev & Hart, 2006). It functions as a catalyst for positive aspects of an online transaction. Given this positive motivation toward online activities, it is more likely that individuals with high PII will conduct activities online, including disclose information online. The privacy calculus model depicts a direct relationship from PII to intention to disclose information. While PII would seem to have the ability to minimize risk perception and amplify the interpretation of potential benefits, no other relationships between PII and other constructs are included in the model. Consequently, I hypothesize that:

H12. Personal Internet Interest (PII) will show a positive relationship with the individual’s intention to disclose information online.
Finally, while the three experimental treatments are analyzed in this study as having a direct influence on the variables of the privacy calculus, it is also possible that these constructs interact to exert an influence on the outcome variables. Specifically, privacy assurances, a positive influence, could have a greater effect on trust, another positive construct in the model, when there is more need for assurances. For example, assurances may have a greater influence on trust when control over information is low, or when information sensitivity is high. Alternatively, high information sensitivity and low personal control could create contexts where privacy assurances are ineffective. This research should provide insight into these previously, unexamined relationships.

3.4 Study Design

A 2x2x2, between subjects, factorial experimental design was employed to test the research model. The three treatments of privacy assurances, information sensitivity and control, were manipulated at high and low levels. A pre-survey was used to capture demographic information (including age and gender) as well as control variables of interest (e.g., prior privacy concerns and agreeableness). The experimental treatments were operationalized through a fictitious website, with eight different versions of the website developed to represent the experimental treatments. A post-survey was used to measure dependent variables of interest, including privacy concerns, risk, trust, and intention to disclose. Descriptions of the participants, experimental process, website, and scales are provided in the sections below.
3.4.1 Participants

After receiving IRB approval, participants were recruited for this study via Amazon’s Mechanical Turk platform (MTurk), as users of this platform can effectively represent the target population (Steelman et al., 2014). The MTurk sample was filtered to include only adults from the United States of America as this was the target population of the study. Participants had the ability to terminate the study at any point in time. The participants received compensation of $1.50 for completing the questionnaire and website visit, which took them an average time of approximately 8 minutes.

3.4.2 Experimental Process and Construct Operationalization

Participants who accepted the MTurk invitation were directed to a Qualtrics questionnaire. After completing the pre-survey section, they were randomly assigned to the experimental website for one of two companies. The instructions for using the website described the services offered by the company; how user’s information would be used and shared with others; and the user’s ability to control that sharing of information. These two different companies corresponded to the high and low forms of the information sensitivity manipulation. The first company website, Infomedical.com (high information sensitivity), offers its customers the collection and storage of personal medical information, through an accessible, centralized repository. The second company website, Infomechanic.com (low information sensitivity), portrays a company which specializes in the collection and storage of a person’s vehicle information through an accessible and centralized repository. Privacy assurances were manipulated via the use of privacy seals and privacy statements within the websites. Figure 3.3 below depicts the high privacy assurances condition for both InfoMedical.com and InfoMechanic.com.
Figure 3.4 (below) shows the corresponding landing pages under the low privacy assurances condition.

The control conditions were implemented through the company descriptions provided in the experimental instructions and materials, as described below. In summary, the privacy assurances treatment was implemented through the company website designs;
the information sensitivity treatment was implemented through the company description in the experimental instructions and on the company websites; and the control treatment was implemented through the company description in the experimental instructions.

The experimental instructions and company descriptions are provided in Appendix A of this chapter for two different combination of treatments (A1: high sensitivity and high control and A2: low sensitivity and low control). The treatment combinations of high sensitivity and high control (A1) were operationalized through the use of the company context, Info-Medical.com, and a control scenario where the participant could control which health information would be shared with designated third parties. The “Company Information” and “Sharing Your Information” sections of the experimental materials implemented these treatment levels as shown in Appendix A. The treatment combinations of low sensitivity and low control (A2) were operationalized through the use of the company context, Info-Mechanical.com, and a control scenario where the participants were given no control over their health information, which was automatically shared with designated third parties.

Scales for all measured constructs used in the study were adapted from the literature and are shown in Table 3.1. The scale sources and end points are also provided.
### Table 3.1 - Survey Items

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Prior Privacy Violations</strong> – Categorical (yes vs. no)</td>
<td>PRIOR To your knowledge, has your personal online information been compromised in the past?</td>
</tr>
</tbody>
</table>
| **Personal Internet Interest** – (Dinev & Hart, 2006) – 7pt. Likert scale | PII1 I find that personal interest in the information that I want to obtain from the Internet overrides my concerns of possible risk or vulnerability that I may have regarding my privacy.  
PII2 The greater the interest to obtain a certain information or service from the Internet, the more I tend to suppress my privacy concerns.  
PII3 In general, my need to obtain certain information or services from the Internet is greater than my concern about privacy. |
| **Agreeableness** – (Donnellan et al., 2006) – 5pt. Likert scale | AGREE1 I sympathize with others’ feelings.  
AGREE2 I am not interested in other people’s problems (r)  
AGREE4 I am not really interested in others. (r) |
| **Privacy Concerns** – Adapted from (Dinev et al., 2006) – 7pt. Likert scale | PC1 I am concerned that the information I submit to this company website could be misused.  
PC2 I am concerned that a person can find private information about me on this company website.  
PC3 I am concerned about submitting information on this company website, because of what others might do with it.  
PC4 I am concerned about submitting information on this company website, because it could be used in a way I did not foresee.  
PC5 Overall, to what degree are you concerned about the privacy of the information you would provide to this company website? |
| **Perceived risk** (Dinev & Hart, 2006) – 7pt. anchored scale: Very Low Risk – Very High Risk. Intro: “What do you believe is the risk for users of this company website due to the possibility that...” | RISK1 The information you provide to this company could be sold to third parties.  
RISK2 Your personal information submitted to this company website could be misused.  
RISK3 Your personal information submitted to this company website could be made available to unknown individuals or companies without your knowledge.  
RISK4 Your personal information submitted to this company website could be made available to government agencies. |
| **Trust** (Hong & Thong, 2013) – 7pt. Likert scale | TRUST1 The company website I visited would be trustworthy in handling my personal information.  
TRUST2 This company's website would keep my best interests in mind when dealing with my personal information.  
TRUST3 The company website would fulfill their promises related to my personal information.  
TRUST4 The company website seems predictable and consistent regarding the usage of my personal information. |
| **Intention to Disclose** – Adapted from (Bansal et al., 2010) – 7pt. Likert scale | ITD1 How likely are you to use this company's information storage service? |
3.5 Analysis and Results

A total of 196 complete responses were collected for the study, with all responses used and no observations discarded. Attention checks, such as disguised questions giving specific directions and a Stroop test, were incorporated into the survey instrument to reduce common method bias as suggested by Fowler, (2009). Descriptive statistics for all measured variables, per treatment, are presented in Table 3.2 below.

Table 3.2 - Mean scores for all variables by treatment

<table>
<thead>
<tr>
<th>Control Variables</th>
<th>High</th>
<th>Low</th>
<th>High</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Assurances</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>High</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information Sensitivity</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>High</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privacy Concerns</td>
<td>3.79</td>
<td>3.49</td>
<td>3.70</td>
<td>4.08</td>
</tr>
<tr>
<td>Perceived Risk</td>
<td>3.58</td>
<td>3.61</td>
<td>3.95</td>
<td>4.28</td>
</tr>
<tr>
<td>Trust</td>
<td>5.03</td>
<td>4.78</td>
<td>4.40</td>
<td>4.87</td>
</tr>
<tr>
<td>Intention to Disclose</td>
<td>4.36</td>
<td>4.67</td>
<td>4.10</td>
<td>4.31</td>
</tr>
<tr>
<td>Control Variables</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Age</td>
<td>39.13</td>
<td>34.54</td>
<td>42.08</td>
<td>41.92</td>
</tr>
<tr>
<td>Gender (M/F)%</td>
<td>75/25</td>
<td>71/29</td>
<td>58/42</td>
<td>60/40</td>
</tr>
<tr>
<td>Prior (1 vs. 2)</td>
<td>1.42</td>
<td>1.50</td>
<td>1.42</td>
<td>1.48</td>
</tr>
<tr>
<td>Personal Internet Interest</td>
<td>4.10</td>
<td>5.08</td>
<td>4.58</td>
<td>4.52</td>
</tr>
</tbody>
</table>

Table 3.2 - Mean scores for all variables by treatment
3.5.1 Manipulation Checks

An analysis of the experimental manipulations was conducted to ensure the effectiveness of the treatments using the manipulation check questions included above in Table 3.1. Manipulation effects were analyzed via MANCOVA in SPSS 28 utilizing the more rigorous method described by Perdue & Summers (1986). This technique observes not only the effect each treatment has on its corresponding manipulation check item but also ‘cross-checks’ potential effects of each treatment on the unrelated items. Significance is expected on the corresponding treatment while non-significance expected on unrelated treatments. As shown in Table 3.3 below, there was a significant difference in the control treatments scores, (3.52_{high}, 1.70_{low}, p-value < .001); the privacy assurance treatments scores, (1.85_{high}, 1.09_{low}, p-value < .001); and the information sensitivity treatments scores, (4.32_{high}, 2.36_{low}, p-value < .001).

Table 3.3 - Manipulation check scores

<table>
<thead>
<tr>
<th>Item</th>
<th>Control</th>
<th>Privacy Assurance</th>
<th>Information Sensitivity</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>p-value</td>
<td>F</td>
<td>p-value</td>
</tr>
<tr>
<td>Item 1 – Control</td>
<td>&lt;.001*</td>
<td>165.575</td>
<td>.171</td>
</tr>
<tr>
<td>Item 2 – Assurance</td>
<td>.236</td>
<td>1.414</td>
<td>&lt;.001*</td>
</tr>
<tr>
<td>Item 3 – Sensitivity</td>
<td>.738</td>
<td>.112</td>
<td>.240</td>
</tr>
</tbody>
</table>

*p-value < 0.001

3.5.2 Measurement Validity and Reliability

Reliability analysis was performed using Cronbach’s alpha, and exploratory factor analysis (EFA) was conducted using Varimax rotation with Principal Components Analysis. Both procedures were performed via IBM SPSS 28. Table 3.5 provides the reliability analysis results, with all Cronbach Alpha scores exceeding 0.88 suggesting
strong reliability (Cortina, 1993; Nunnally, 1978). Support for the convergent and
discriminant validity of the constructs is also provided in Table 3.5, where the average
variance extracted (AVE) scores are well above 0.5, suggesting good convergent validity
(Podsakoff et al., 2003), and the square root of the AVE scores for all constructs are
higher than the correlation values with the other constructs, demonstrating satisfactory
discriminant validity (Mackenzie et al., 2011). The EFA results (Table 3.4) also show
good convergent and discriminant validity\(^1\), with all factor loadings above 0.72 and all
cross-loading differences no larger than 0.3, meeting the standard for discriminant

Table 3.4 - Study items’ loadings and cross-loadings from EFA.

<table>
<thead>
<tr>
<th>Component</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>PII1</td>
<td>0.065</td>
<td>-0.140</td>
<td>-0.059</td>
<td>0.896</td>
<td>-0.132</td>
</tr>
<tr>
<td>PII2</td>
<td>0.114</td>
<td>-0.006</td>
<td>-0.033</td>
<td>0.901</td>
<td>-0.050</td>
</tr>
<tr>
<td>PII3</td>
<td>0.083</td>
<td>-0.110</td>
<td>-0.115</td>
<td>0.916</td>
<td>-0.112</td>
</tr>
<tr>
<td>AGREE1</td>
<td>0.136</td>
<td>0.099</td>
<td>0.024</td>
<td>-0.150</td>
<td>0.812</td>
</tr>
<tr>
<td>AGREE2r</td>
<td>-0.091</td>
<td>0.053</td>
<td>0.017</td>
<td>-0.085</td>
<td>0.935</td>
</tr>
<tr>
<td>AGREE4r</td>
<td>-0.092</td>
<td>0.030</td>
<td>-0.005</td>
<td>-0.047</td>
<td>0.922</td>
</tr>
<tr>
<td>GPC1</td>
<td>-0.388</td>
<td>0.832</td>
<td>0.256</td>
<td>-0.104</td>
<td>0.039</td>
</tr>
<tr>
<td>GPC2</td>
<td>-0.307</td>
<td>0.820</td>
<td>0.290</td>
<td>-0.088</td>
<td>0.045</td>
</tr>
<tr>
<td>GPC3</td>
<td>-0.385</td>
<td>0.843</td>
<td>0.221</td>
<td>-0.071</td>
<td>0.052</td>
</tr>
<tr>
<td>GPC4</td>
<td>-0.364</td>
<td>0.824</td>
<td>0.285</td>
<td>-0.072</td>
<td>0.080</td>
</tr>
<tr>
<td>GPC5</td>
<td>-0.352</td>
<td>0.838</td>
<td>0.240</td>
<td>-0.117</td>
<td>0.123</td>
</tr>
<tr>
<td>RISK1</td>
<td>-0.468</td>
<td>0.293</td>
<td>0.709</td>
<td>-0.052</td>
<td>0.086</td>
</tr>
<tr>
<td>RISK2</td>
<td>-0.379</td>
<td>0.402</td>
<td>0.729</td>
<td>-0.068</td>
<td>0.050</td>
</tr>
<tr>
<td>RISK3</td>
<td>-0.423</td>
<td>0.400</td>
<td>0.720</td>
<td>-0.053</td>
<td>0.095</td>
</tr>
<tr>
<td>RISK4</td>
<td>-0.213</td>
<td>0.269</td>
<td>0.772</td>
<td>-0.143</td>
<td>-0.102</td>
</tr>
<tr>
<td>TRUST1</td>
<td>0.836</td>
<td>-0.292</td>
<td>-0.258</td>
<td>0.034</td>
<td>-0.091</td>
</tr>
</tbody>
</table>

\(^1\) During pilot tests, one item from the Agreeableness (Donnally, 2006) scale showed poor convergent and
discriminant validity. This item read “\textit{I feel other people’s emotions.}” Upon further analysis, we argue that
the wording is vague in that it can be interpreted as an actual feeling of others’ emotions and not related to
being empathetic to others’ feelings. This item was dropped from the study.
Table 3.5 - Reliability, Correlations and AVE

<table>
<thead>
<tr>
<th></th>
<th>Alpha</th>
<th>AVE</th>
<th>PII</th>
<th>AGREE</th>
<th>PC</th>
<th>RISK</th>
<th>TRUST</th>
<th>ITD</th>
</tr>
</thead>
<tbody>
<tr>
<td>PII</td>
<td>0.911</td>
<td>.775</td>
<td>0.880</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AGREE</td>
<td>0.883</td>
<td>.733</td>
<td>-0.223</td>
<td>0.887</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PC</td>
<td>0.972</td>
<td>.877</td>
<td>-0.265</td>
<td>0.167</td>
<td>0.936</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RISK</td>
<td>0.923</td>
<td>.762</td>
<td>-0.243</td>
<td>0.138</td>
<td>0.780</td>
<td>0.873</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TRUST</td>
<td>0.949</td>
<td>.825</td>
<td>0.219</td>
<td>-0.167</td>
<td>-0.706</td>
<td>-0.751</td>
<td>0.908</td>
<td></td>
</tr>
<tr>
<td>ITD</td>
<td>0.954</td>
<td>.877</td>
<td>0.221</td>
<td>-0.063</td>
<td>-0.656</td>
<td>-0.655</td>
<td>0.831</td>
<td>0.936</td>
</tr>
</tbody>
</table>

Square root of the AVE is expressed in the bolded diagonal

Additionally, a confirmatory factor analysis (CFA) was performed and the fit statistics (CFI: 0.978; RMSEA: 0.053; SRMR: 0.036), all exceed the recommended thresholds in the literature (Kline & Santor, 2016) which suggests strong discriminant and convergent validity as well as good fit of the data for the measurement model.

3.5.3 Analysis – Hypothesis Testing

The hypotheses in the research model are analyzed using two statistical techniques given the inclusion of treatment variables and a sequence of latent variables in the research model. First, a multivariate analysis of covariance (MANCOVA) is utilized to test the effect of all independent variables, including experimental treatments and control variables, on all four endogenous variables in the model. While this form of analysis includes all measured variables, it does not consider the relationships among the
endogenous variables, which represent the privacy paradox portion of the model. A structural regression model using MPlus is also conducted to better assess the relationships among all latent variables in the research model.

The MANCOVA analysis is shown in Table 3.6 below. The hypothesized effects of control on privacy concerns ($3.89_{\text{high}}, 4.95_{\text{low}}, \text{p-value} < .001$); perceived risk ($3.70_{\text{high}}, 4.82_{\text{low}}, \text{p-value} < .001$), and trust ($4.73_{\text{high}}, 3.87_{\text{low}}, \text{p-value} < .001$) were all significant, supporting H1, H2 and H3, respectively. Information sensitivity showed a significant effect on privacy concerns ($4.74_{\text{high}}, 4.11_{\text{low}}, \text{p-value} .008$), supporting H4, but a non-significant effect on perceived risk ($4.39_{\text{high}}, 4.15_{\text{low}}, \text{p-value} .266$), thus H5 was not supported. Finally, privacy assurances had a significant effect on trust ($4.67_{\text{high}}, 3.92_{\text{low}}, \text{p-value} < .001$), supporting H6.

PII had a significant effect on all dependent variables, including privacy concerns (p-value < .001), perceived risk (.002), trust (p-value .005), and intention to disclose information (p-value .014). The significant relationship between PII and intention provides preliminary support for H12, and will be further tested within the structural regression analysis presented in the next section. The control variables of age, gender, prior privacy violations and agreeableness were also included in the model. Age had a marginally significant effect on both perceived risk (p-value .059) and privacy concerns (p-value .078), with older individuals perceiving a larger degree of risk compared to younger individuals and having greater privacy concerns. These age effects are consistent with previous findings in the extant literature (Li, et al., 2014). Gender had a significant effect on privacy concerns (p-value .028) but not risk (p-value .571), with females
reporting higher concerns. The agreeableness trait does not appear to have a significant
effect on any of the dependent variables.

Table 3.6 - MANCOVA Results

<table>
<thead>
<tr>
<th>Dependent Variables</th>
<th>Privacy Concerns</th>
<th>Perceived Risk</th>
<th>Trust</th>
<th>Intention to Disclose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>F</td>
<td>p-value</td>
<td>F</td>
<td>p-value</td>
</tr>
<tr>
<td>Age</td>
<td>3.149</td>
<td>0.078</td>
<td>3.603</td>
<td>0.059</td>
</tr>
<tr>
<td>Gender</td>
<td>4.896</td>
<td>0.028*</td>
<td>0.322</td>
<td>0.571</td>
</tr>
<tr>
<td>Prior</td>
<td>2.140</td>
<td>0.145</td>
<td>5.368</td>
<td>0.022*</td>
</tr>
<tr>
<td>PII</td>
<td>12.005</td>
<td>&lt;0.001**</td>
<td>10.174</td>
<td>0.002**</td>
</tr>
<tr>
<td>AGREE</td>
<td>0.480</td>
<td>0.489</td>
<td>0.160</td>
<td>0.690</td>
</tr>
<tr>
<td>Control</td>
<td>14.459</td>
<td>&lt;0.001**</td>
<td>20.682</td>
<td>&lt;0.001**</td>
</tr>
<tr>
<td>Assurance</td>
<td>5.536</td>
<td>0.020*</td>
<td>3.187</td>
<td>0.076</td>
</tr>
<tr>
<td>Sensitivity</td>
<td>7.286</td>
<td>0.008**</td>
<td>1.245</td>
<td>0.266</td>
</tr>
<tr>
<td>Control x Assurance</td>
<td>1.018</td>
<td>0.314</td>
<td>1.934</td>
<td>0.166</td>
</tr>
<tr>
<td>Control x Sensitivity</td>
<td>0.559</td>
<td>0.456</td>
<td>1.285</td>
<td>0.258</td>
</tr>
<tr>
<td>Assurance x Sensitivity</td>
<td>0.711</td>
<td>0.400</td>
<td>0.790</td>
<td>0.375</td>
</tr>
<tr>
<td>Control x Assurance x Sensitivity</td>
<td>1.663</td>
<td>0.199</td>
<td>0.384</td>
<td>0.536</td>
</tr>
</tbody>
</table>

* significant at the 0.05 p-value level; ** significant at the 0.01 p-value level

The MANCOVA analysis also revealed a significant interaction of control and
privacy assurances on trust. A post-hoc analysis of the interaction, as shown in table 3.7,
suggests that privacy assurances are most effective when users have low control over the
use of their data. Under a low control condition, the effect that assurances have on trust is
much (almost three times) larger than the comparable effect under a high control
condition. Expressed differently, this data pattern seems to suggest that when control is
low, the presence of assurance becomes three times as powerful in trust formation as it is
under the presence of high control.
Table 3.7 - Interaction effects of Control and Assurance on Trust

<table>
<thead>
<tr>
<th>Control Condition</th>
<th>Assurance Condition</th>
<th>Mean Score</th>
<th>Differential</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>High</td>
<td>4.9</td>
<td>0.4</td>
</tr>
<tr>
<td>High</td>
<td>Low</td>
<td>4.5</td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td>High</td>
<td>4.45</td>
<td>1.17</td>
</tr>
<tr>
<td>Low</td>
<td>Low</td>
<td>3.28</td>
<td></td>
</tr>
</tbody>
</table>

3.5.4 Structural Regression Model

A structural equation model (SEM) analysis was employed to perform a more rigorous analysis of the relationships among the latent variables in the study. Figure 3.5 presents the hypothesized relationships among the latent variables and displays path significance and explained variance. This model also corresponds to the original privacy calculus model proposed by Dinev & Hart (2006). Perceived risk was proposed as having an impact on privacy concerns, trust, and intention to disclose information. First, the hypothesized positive effect of perceived risk on privacy concerns is highly significant (p-value = 0.000; standardized path coefficient = 0.791) in support of H7. Second, risk did not have a direct effect on intention to disclose information (p-value = 0.716; standardized path coefficient = 0.034) failing to provide support for H10. Lastly, the anticipated effect of risk on trust is confirmed (p-value = 0.000; standardized path coefficient = 0.765), providing strong support for H8 of the model. Additional analysis was performed on the model, and it was determined that while perceived risk and intention to disclose information were significantly correlated, with the other constructs and paths in the model, the effect of perceived risk was fully mediated.

Next, the hypothesized effect of privacy concerns on intention to disclose (p-value = 0.039; standardized path coefficient = 0.164) shows support for H9. The effect of trust
on the intention to disclose information is also strongly significant (p-value = 0.000; standardized path coefficient = 0.746), providing evidence for support of H11. The hypothesized relationship between personal internet interest and information to disclose information is not significant (p-value = 0.568; standardized path coefficient = 0.027) failing to provide support for H12. Additional analysis was conducted to determine if PII was related to other constructs in the privacy calculus model. PII had a significant relationship with perceived risk, but with no other constructs in the model.

![Figure 3.5 - Structural model. Dotted paths are non-significant.](image)

Table 3.8 summarizes the model fit indices for the structural model and provides evidence of good fit of the data for the model as established by Kline & Santor, (2016).

<table>
<thead>
<tr>
<th>Test</th>
<th>Value</th>
<th>Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normed Chi Square</td>
<td>1.56</td>
<td>&lt; 2 is ideal; &lt; 3 is acceptable</td>
</tr>
<tr>
<td>CFI</td>
<td>0.978</td>
<td>Above &gt;.9 acceptable;</td>
</tr>
<tr>
<td>RMSEA</td>
<td>0.053</td>
<td>Between .05 and .08 is adequate</td>
</tr>
<tr>
<td>SRMR</td>
<td>0.036</td>
<td>&gt;.1 indicates poor fit</td>
</tr>
</tbody>
</table>
Based on the analysis conducted with MANCOVA and SEM, as reported above, a summary of all hypotheses results is presented in table 3.9 below:

Table 3.9 - Hypotheses results

<table>
<thead>
<tr>
<th>Hypotheses</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>H1 Perceived control will be negatively related to privacy concerns.</td>
<td>Supported</td>
</tr>
<tr>
<td>H2 Perceived control will be negatively associated with the corresponding perceived risk by an internet user.</td>
<td>Supported</td>
</tr>
<tr>
<td>H3 Perceived control will be positively associated with the trust of the individual towards the company website.</td>
<td>Supported</td>
</tr>
<tr>
<td>H4 Information sensitivity will be positively related to the resulting individual's privacy concerns.</td>
<td>Supported</td>
</tr>
<tr>
<td>H5 Information sensitivity will be positively associated with the individual’s perceived risk.</td>
<td>Not supported</td>
</tr>
<tr>
<td>H6 Privacy assurances will show a positive relationship with degree of trust towards the site.</td>
<td>Supported</td>
</tr>
<tr>
<td>H7 Perceived risk will be positively related to an individual’s privacy concerns.</td>
<td>Supported</td>
</tr>
<tr>
<td>H8 Perceived risk will negatively impact the trust an individual has for an online vendor.</td>
<td>Supported</td>
</tr>
<tr>
<td>H9 Privacy concerns will be negatively related to an individual's intention to disclose information.</td>
<td>Supported</td>
</tr>
<tr>
<td>H10 An individual's perceived risk will be negatively related to their intention to provide information.</td>
<td>Not supported</td>
</tr>
<tr>
<td>H11 Trust will be positively associated to the individual’s intention to disclose information.</td>
<td>Supported</td>
</tr>
<tr>
<td>H12 Personal Internet Interest (PII) will show a positive relationship with the individual’s intention to disclose information online.</td>
<td>Not supported</td>
</tr>
</tbody>
</table>

3.6 Discussion and Contributions

3.6.1 Theoretical Contributions

The present study created a replication of the privacy calculus model and extended it via a 2x2x2 factorial design experiment. Six hypotheses are unique to the
study and the other six provided a needed confirmation of the privacy calculus model in a
different context. Of the unique aspect of this study, the control construct is demonstrated
to be a powerful antecedent to privacy concerns, perceived risk, and trust just as
hypothesized. In addition to privacy conceptualizations that include the control
dimension, such as Malhotra et. al., (2004), separate operationalizations of control should
be included in privacy research, along with theories that consider control, to better inform
future examinations of privacy concerns and related outcomes. The first important
theoretical or conceptual contribution of this study lies in the hypothesized effects that
control has on privacy-related dependent variables. The role of control in the privacy
phenomena appears to have a wide set of effects on different parts of the model.
Considering that the three outcome variables in these relationships are all important
antecedents to intention to disclose in the privacy calculus model, this finding holds great
promise for research.

At the same time, information sensitivity is shown to be a significant antecedent
to privacy concerns. Given the prominence of the privacy concerns construct in the
literature, it is important to consider this relationship for future research endeavors. The
specific insight gained is that the health information sensitivity, or context, is shown to
have an important effect in the formation of individual privacy concerns when these
concerns are measured as a context-dependent variable. No other examples of this finding
have been found in the literature arising from an experimental setting. This not only
showcases the importance of considering information sensitivity as an antecedent to
privacy concerns, but also contributes to the privacy literature by showing that privacy
cconcerns are a function of context too, when compared to non-health-related contexts.
Finally, privacy assurances such as seals of privacy warranty or statements regarding the management of information on a website, are antecedents of the degree of trust an individual feels for the online vendor. Together with individual access to control of information, the presence of privacy assurances can effectively ameliorate the effects of perceived risks and the privacy concerns of users.

Among the relations coming from the privacy calculus model, privacy risk is shown to be of pointed importance in the model as an important antecedent to both the privacy concerns as well as trust (negative relationship). Consequently, both privacy concerns and trust are shown to be effective antecedents to the intention to disclose information, confirming the relevance of the original privacy calculus model. Given the observed lack of direct effect of risk on the intention to disclose, additional analysis was performed and showed a full mediation of perceived risk by privacy concerns. In the original privacy calculus study (Dinev & Hart, 2006), perceived risk was partially mediated, and thus these findings are not surprising. Further exploration of the relationship between perceived risk and the intention to disclose information could help identify when a stronger mediation is likely.

In this application of the privacy calculus model, I also examined the direction of the relationship between risk and trust. Support was previously provided for the notion that risk is a proper antecedent to trust. Both the SEM model fit statistics, as well as the path analysis provide support for perceived risk leading to trust. Additional analysis was also conducted to better understand the lack of a direct relationship between personal internet interest and users’ intention to disclose information. The analysis revealed that PII was related to perceived risk, but no other constructs in the model. We also reviewed
the means for PII in the current study compared to the original Dinev & Hart (2006)
study and found that the average PII was 4.46 as compared to the mean of 3.39 in 2006.
It is not surprising that PII may have increased during the past 15 years, especially given
the effects of the pandemic on online shopping and communication. With higher levels of
PII, and more homogeneity of PII levels, the relationship between PII and intention to
disclose may have diminished. Further investigation of the changing levels and influence
of personal internet interest are warranted.

Of the control variables used in the research, age and gender show tenuous effects
on privacy concerns and risk, just as predicted by the extant literature with older
individuals displaying larger measures of privacy concerns and risk; Correspondingly,
females show a slightly higher degree of privacy concerns. Prior privacy violations is also
shown to affect the participants’ perceived risk and trust with individuals who have
experienced a prior privacy violation interpreting a higher degree of risk and lower
measure of trust, which is also consistent with other studies. One particular exception of
the expected effects is shown by the lack of effects that the personality trait agreeableness
has on any of the dependent variables identified by our research model. While two
prominent studies consistently found agreeableness to be a significant antecedent of
privacy concerns (Bansal et al., 2016; Junglas et al., 2008), they both showed the
opposite effect. Our study failed to provide evidence for significant effects of
agreeableness as an antecedent of any dependent variables including privacy concerns.
Since the literature included opposite effects in two different studies (Bansal et al., 2016;
Junglas et al., 2008), a potential explanation is that control variables used in the current
study are more comprehensive and have better explanatory power when compared to the
examples in the literature which included only a limited set of control variables. Further analysis of agreeableness and other personality traits is warranted, as it is intuitive to think that a personality trait might influence the privacy individuals expect from online vendors.

Context-specific privacy concerns, while an important antecedent to the intention to disclose information, is not a powerful predictor, especially when compared to trust. Consistently with the findings in the extant literature, trust appears to be a powerful predictor of the individual’s intention to disclose information.

### 3.6.2 Practical Implications

Information sensitivity is shown to negatively impact users’ privacy concerns. For practitioners dealing with customer’s sensitive data, it would be important to understand that even a notion of control can have a powerful influence on the individuals’ intention to disclose information. Online artifacts are more capable of incorporating specialized tools to maximize user control, and these increased levels of control are not only feasible, but apparently necessary if we want to maximize user/client participation and self-disclosure.

Another important contribution from this research lies in the effect of privacy assurances on the resulting trust an individual has for an online vendor. Just as is the case with control, providing privacy assurances to customers/users is shown to influence the degree to which individuals trust the online vendor (Lowry et al., 2014). This notion has seen some debate in IS, mostly concerning the conceptualization of assurances as well as the context in which these are used (Hui et al., 2007). Despite this debate, the clear
contribution of this study lies in the fact that, in general, privacy assurances can influence the degree of trust a user develops for an online vendor’s site. Given the widely accepted importance of trust in the privacy phenomena, the confirmed effect of assurances expands our understanding of its relationship with trust. It also provides a clear guideline to practitioners who might consider incorporating different forms of privacy assurance when promoting and/or presenting their products and services online.

This study also explored the possibility of interactions between privacy assurances and control, and information sensitivity. A significant interaction was found between control and assurances on the trust formation of the participants. In settings where control cannot be fully granted to online users, the presence of privacy assurances provides support for developing the needed trust required to encourage participation and/or adoption. A similar interaction between assurances and information sensitivity was not significant. Further examination of the effectiveness of privacy assurances under differing conditions of control and information sensitivity is warranted and may explain some mixed results in prior research on privacy assurances.

The causal relationship of risk being the antecedent to trust was supported by this study’s results. Although no comparative analysis of the role of risk with regards to trust is included in this study, that precise design could constitute a valuable next step in the analysis of the relationship between these constructs where the mediating role of risk between antecedents and trust is more fully examined.
3.7 Conclusion and Limitations

As with any experiment, external validity of the findings and results can be a concern with the present study. Even though they were notified that the exercise portrayed fictitious online companies, the notion that the website is not an actual service from a real company can potentially affect the participant’s input. Additionally, actual users of sites like the ones portrayed by the experiment would logically display a higher degree of interest in such services and might, therefore, display different levels of the measures captured by the survey. However, as is true for all research experiments, the comparative analysis between treatments is what represents the most valuable contributions of this study in pursuit of internal validity.

The present study utilized an experimental setting to test the effects of three important antecedents to privacy-related outcomes (privacy assurances, control and information sensitivity), integrated within a widely accepted theoretical model in IS privacy research: the privacy calculus model. While not all of the proposed relationships were supported, several important findings supported and discussed. Among them, the most important include the confirmation of the importance of control in the privacy setting; the important positive effect of assurances (via trust) on the intention to disclose information and the importance of information sensitivity as a relevant source of privacy concerns for individuals. Finally, a complementary influence of control and privacy assurances on trust formation was discovered by this study. All of these not only are important contributions to the body of knowledge but also represent opportunities for future research in IS privacy studies.
Some of the most important findings of this study present clear opportunities for future research. First, given the demonstrated importance of the control construct in this study, a more elaborate conceptualization of control as well as a theoretical background that allows for this inclusion is needed. Second, while the directional relationship between risk and trust seems supported by the present research model, a comparative analysis of this relationship could further our understanding of said relationship and can be adopted by future research. Third, given the apparent relevance of information sensitivity pertaining to health information, a study carried out entirely in a health setting can further the application and analysis of privacy in a highly relevant context. Fourth, personal internet interest (Dinev & Hart, 2006) and other online and privacy-related constructs may have changed substantially over the last 15 years, given the general growth in e-commerce; increased use of electronic records; and the many changes in online activity brought about from the pandemic. Research is needed to both document the changes that have occurred and to be better measure and manage current privacy concerns and information disclosure behaviors. Such behaviors may have significantly changed as the world shifted to a more remote and less mobile version of life before the pandemic.
Appendix A: Website descriptions and instructions to experiment participants.

A1. Company 1: InfoMedical.com (High information sensitivity)

Assume you are interested in a service that stores your health-related information. You come across the home page of Info-Medical.com, a Health Information Management Company. You are now considering this vendor for storage of your personal health information. Please read the descriptive information below and then answer a few questions about this company.

Company Information: Info-Medical.com collects your personal medical and health-related information. The service this company offers is to keep your records in a central location so health providers have direct, quick access to all of your health and medical history and you have the ability to see it and update it as new information becomes available. Healthcare providers can also update your health information as it changes. In case of an emergency and in case you can't recall the requested information, this company would be able to provide fast access to your complete health information. Whenever you change your healthcare provider, a few-clicks will grant them access to your health history avoiding you having to fill out paper forms every time you go to a new provider.

Sharing Your Personal Information: (high control) Info-Medical.com provides you with complete control over the use and distribution of your personal health information. We will only share your contact information with third-party providers and business partners. No other information will be shared with other parties unless you authorize Info-Medical.com (opt-in) to share more information.
A2. Company 2: InfoMechanic.com (Low information sensitivity)

Assume you are interested in a service that stores your vehicle-related information and have come across the home page of Info-Mechanic.com, a Vehicle Information Management company. You are now considering this vendor for storage of your vehicle's information. Please read the descriptive information below and then answer a few questions about this company.

Company Information: Info-Mechanic.com collects your vehicle maintenance/repair history and information. The service this company offers is to keep all of your vehicle's records in a central location so mechanics and car dealers have direct, quick access to your vehicle's history and you have the ability to see it and update it as new information becomes available. Auto professionals can also update your vehicle's information as it changes. When you want to sell your (or buy someone else's) vehicle, this company provides easy, fast access to the vehicle's history and information. Such service can help owners maximize the value of their vehicles and lets buyers assess the fair price to pay for a car.

Sharing Your Personal Information: (low control) Info-Mechanic.com will automatically share your contact information and your personal health information with related third-party providers or business partners. When you sign-up for this service, you are required to authorize the sharing of your personal health information.
CHAPTER 4
MAXIMIZING PRIVACY CONTROL: THE ROLE OF PERSONAL, PROXY AND COLLECTIVE CONTROL IN ONLINE COMMUNITY INFORMATION DISCLOSURE

4.1 Introduction

The era of the Internet has opened the floodgates for the transmission and analysis of enormous amounts of personal data. We regularly share our personal information while shopping online, using social networks, or participating in online communities (Goh et al., 2016), while the privacy of our personal information remains a significant concern. Early information systems (IS) research on privacy concerns and online information disclosure (Margulis, 1977; J. Smith et al., 1996) demonstrated the need to study and understand the psychology of privacy, and it continues to be an active research area, with important practical implications (Belanger & Crossler, 2011) in a range of highly relevant contexts.

Online communities present an interesting context for the study of privacy concerns, because such communities provide the most benefits when their members readily share personal information and learn from one another (Munson et al., 2013). Among different types of online communities, online health communities (OHCs) offer distinct settings for researchers to advance our understanding of the interplay of privacy concerns and online information disclosure. In particular, OHCs provide users with the ability to learn more about their own health conditions and experiences by joining communities where personal health information flows freely (J. Li, 2013; Munson et al., 2013). Although such online communities offer a rich source of valuable, personally
relevant information, including medical referrals, expert advice, and empathy, access to these valuable resources is often predicated on participants joining the community and sharing their own highly personal, health information (Vaala et al., 2017). In joining such a community, participants lose some level of control over their personal, sensitive information and how it is used or shared within the community. Individuals need assurance and encouragement to join these communities, but guidance on how to do so is often limited (e.g., Zhang et al., 2018). As a result, information privacy and disclosure remain a challenge in the development of a successful OHC.

In IS research, privacy calculus is commonly applied in studies of information disclosure (Dinev & Hart, 2006; Kordzadeh & Warren, 2017), to describe how individuals assess the costs and benefits of disclosing personal information in a rational manner. Similarly, the privacy paradox describes how disclosure of personal information can occur in an irrational manner (Awad & Krishnan, 2006). While these theoretical perspectives explain how individuals contemplate privacy issues and how their concerns of privacy influence online self-disclosure decisions, they do not provide adequate guidance on how to assist users in making risk assessments. In light of this, research on privacy concerns and assurances holds promise for developing interface design elements that convey relevant privacy information to users and help them to better assess their risks in sharing personal information with an online community (J. Li, 2015; Lowry et al. 2012).

One of the recurrent themes in prior research on privacy and privacy assurance is control over one’s personal information. As users perceive greater risk when they have less control over how their personal information is used (Belanger et al., 2002), there is a
strong connection between control and privacy (Westin, 1967), and control is believed to shape privacy concerns (Smith and Dinev, 2011). Research on control from the agentic perspective of social cognitive theory (Bandura, 2001) holds promise for a more nuanced understanding of privacy concerns (Xu et al., 2012). The agentic perspective describes three modes of control, including personal, proxy and collective, and all three of these different modes of control are highly applicable to online communities such as OHCs. Personal control is applicable to all contexts, including OHC. Proxy control, which refers to the third parties which provide oversight or requirements, aligns with regulatory agencies in a healthcare context. Collective control applies to a community or group of like-minded individuals, which is inherent in online communities.

In this research, an experimental study is conducted in the context of OHCs to examine how privacy assurances can be offered through different control mechanisms and how they can in turn influence perceived risk, trust, and disclosure intentions. In particular, the above-mentioned modes of control are presented in an experimental website to examine how personal, proxy, and collective control assurances affect users’ willingness to disclose their personal information to the community. Global privacy concerns and other known antecedents to perceived risk and disclosure intentions are controlled. Personal internet interest (PII) (Dinev & Hart, 2006) is incorporated to examine motivation as an important determinant of disclosure intentions. The results show that personal and collective control influence perceived risk, while personal and proxy control influence trust, and that personal internet interest influences perceived risk and intention to disclose in an OHC context. Several mediating relationships are supported with PII leading to risk, and risk leading to trust. These research findings
expand our understanding of the role of control in studies of privacy and provide several important implications for the interface designs of OHCs and online communities in general.

4.2 Theoretical Background

4.2.1 Privacy and Control

In this section, the definitions and measures of privacy concerns are introduced. A review of prior research on privacy concerns is presented, including privacy calculus, perceived risk, trust, information disclosure, and privacy assurance. The agentic perceptive of privacy control is then introduced for the present research and the rationales for choosing this theoretical perspective on control are offered.

4.2.2 Privacy & Privacy Concerns

Information Systems (IS) has been interested in issues of privacy for some time. An early seminal work on privacy defines it as the level of control one has over one’s personal information (Westin, 1967). Many of the working definitions of privacy found in the field continue to include the concept of control (Belanger & Crossler, 2011), but empirical studies of privacy have defaulted to concern for information privacy (CFIP) as a proxy for privacy. First proposed by Smith et al. (1996), CFIP was conceived as a scale consisting of four sub-dimensions: concerns for information errors, secondary use, unauthorized access, and collection. This 4-dimensional, 15-item construct was validated by Stewart and Segars (2002) and has been used commonly in privacy studies. A more contemporary variation on the measurement of privacy has been offered by Malhotra et al. (2004). Their construct, internet users' information privacy concerns, consists of three
dimensions: collection, control, and awareness of privacy practices. As an alternative to their original measurement instrument, the authors also proposed a more parsimonious, single-dimensional scale to measure privacy concerns: the *global information privacy concern* (GIpc) scale.

### 4.2.3 Risk and Trust in Privacy Studies

The IS literature has noted that risk and trust are inevitably interwoven as important beliefs that are highly relevant to the study of privacy (Jarvenpaa & Tractinsky, 1999). Perceived risk is defined as the extent to which an individual believes that there is a high potential for loss associated with the release of personal information (Featherman & Pavlou, 2003; Malhotra et al., 2004; H. J. Smith et al., 2011), and the sharing and use of data online is inherently associated with risk (H. J. Smith et al., 2011). While risk is negatively related to information disclosure, trust is positively related to disclosure. In privacy research, trust is defined as confidence that personal information submitted online will be handled safely (Dinev & Hart, 2006). The importance of perceived risk and trust as salient beliefs and determinants of information disclosure has been documented in prior research. However, the two constructs have also been examined with different nomological networks. For example, in some privacy studies, trust is a determinant of risk (Malhotra et al., 2004; Miltgen & Smith, 2015), while in others, risk is a determinant of trust (Bansal et al., 2010; Dinev & Hart, 2006), or one construct is included in a privacy model without the other one (Jozani et al., 2020; Midha, 2012).
4.2.4 Motivation to Disclose - Personal Internet Interest

Individual traits have been identified as important antecedents to privacy concerns formation and intention to disclose personal information (Bansal et al., 2016; Belanger & Crossler, 2011). “Based on their traits and experiences, people vary in the extent of their privacy concern, which motivates them differently in spending cognitive energy on suitable privacy cues in forming their trust” (Bansal et al., 2016; p. 627). While individual differences such as age and gender have been studied, there has been limited examination of the influence these differences have on intention to disclose. Personal Internet Interest (PII), defined as one’s personal interest or cognitive attraction to Internet content that may override privacy concerns, was shown to be a significant determine of intention to disclose personal information (Dinev & Hart, 2006). Although certain personal characteristics (such as personality) have enjoyed ample analysis in the privacy literature (Bansal et al., 2016; Junglas et al., 2008), PII has not, and could provide unique insight given the focus on motivation to conduct online transactions.

4.2.5 Theory and the Privacy Calculus

Existing IS research has studied online information privacy and information self-disclosure from the theoretical perspectives of the theory of reasoned action (TRA) (Liu et al., 2005), the privacy calculus (Dinev & Hart, 2006), the elaboration likelihood model (Bansal et al., 2015), and the agentic model (Xu et al., 2012). The privacy calculus model, based on TRA, incorporates key privacy-related constructs under the premise that IS users’ intentions to disclose personal information are in part determined by their valuations of both privacy benefits and costs (Dinev & Hart, 2006; Kehr et al., 2015; Kordzadeh & Warren, 2017; Malhotra et al., 2004; Xu et al., 2009). According to the
privacy calculus model, IS users are likely to disclose their personal information online when they perceive the potential benefits of doing so outweigh privacy risks. Empirical tests of the privacy calculus model have found support across a range of IS contexts (Awad & Krishnan, 2006; Kordzadeh & Warren, 2017; T. Li & Unger, 2012; Xu et al., 2009).

4.2.6 Privacy Assurance

Among different strategies for reducing online privacy risks and alleviating privacy concerns, the provision of explicit privacy notices and data policies on an IS application has been regarded as an important way to reassure users that it is safe to disclose their personal information (Bansal et al., 2015; Milne & Culnan, 2004). According to Bansal et al. (2015), privacy assurances refer to “mechanisms that directly or indirectly provide customers with assurances and guarantees that their private information will be protected and kept private by the website.” (p. 625). Such mechanisms are thought to have two functions in addressing privacy risks: 1) they provide proper security protocols for data protection; and 2) they offer effective control measures that help system users detect and defend against potential data breach threats (Mousavizadeh et al., 2016).

Assurances can be interpreted as a diverse set of characteristics of an IS artifact that communicate a sense of privacy to the user (Xu et al., 2011b). Assurances in the extant literature have been operationalized as seals, statements, and cues among others (e.g., Lowry et al., 2012). Although this line of research has offered different views on the effects of privacy assurances, the empirical evidence generally supports a positive
relationship between assurances and information disclosure (Belanger et al., 2002; Hui et al., 2007; Milne & Culnan, 2004).

In their research, Hui et al. (2007) examined the effects of privacy statements and privacy seals on IS users’ information disclosure decisions. The study results suggest that the presence of privacy statements was likely to increase people’s tendency to disclose information online, but the effect of privacy seals on information disclosure was insignificant. Some researchers have found that the existence of privacy assurances could help establish and enhance users’ trust in an IS application, and in turn encourage information disclosure (Bansal et al., 2015; Belanger et al., 2002). Drawing upon the elaboration likelihood model (Petty & Cacioppo, 1986), Lowry et al. (2012) showed that although people’s positive perceptions of privacy assurance could increase their intention to give information online, such perceptions are influenced not only by the presence of privacy statements, but also by web-based cues such as website quality and brand image. Taken together, privacy assurances have largely achieved consensus as being significant influencers on the sense of privacy an individual can derive from the use of an artifact. Nevertheless, there are only a handful of studies available on this research topic. Given that privacy assurances are arguably a direct way in which organizations can communicate their stance on the management of users’ personal information, more research into assurances is necessary.

4.2.7 The Agentic Perspective of Privacy Control

To extend past research on privacy assurances, the present research draws upon social cognitive theory (Bandura, 2001) and focuses on privacy control mechanisms (PCMs) as a special type of privacy assurance in the context of OHCs. Our rationales for
centering on privacy control mechanisms (PCMs) from a social cognitive perspective are three-fold. First, the concept of control is intrinsically entangled with the notion of privacy (Belanger & Crossler, 2011). An in-depth examination of PCMs can help shed some light upon the distinct role of PCMs in influencing individuals’ trust and perceived privacy risks in OHCs. In particular, although information privacy has been defined in many ways, an element recurring in those definitions is some form of control over the secondary use of one’s personal information (Belanger et al., 2002). Given control as an integral part of the conceptualization of information privacy, empirical research on PCMs is much needed for developing an advanced understanding of what effects they can have on individuals’ privacy calculus considerations and information disclosure decisions.

Second, social cognitive theory (Bandura, 2001) is particularly relevant to the present research, because the agentic perspective posited in this theory offers a modern, rich conceptualization of control in online information privacy. Bandura (2001) notes that “the capacity to exercise control over the nature and quality of one’s life is the essence of humanness.” (p. 1). Social cognitive theory explains that the ability of an individual to be involved in any given decision or situation (namely, control exertion) has a powerful cognitive effect on the evaluation of the experience.

Lastly, as noted earlier, the provision of privacy assurances can be manifested in different design aspects of an IS artifact. Similarly, different PCMs in OHCs can have qualitatively different features and characteristics. Social cognitive theory (Bandura, 2001) offers a unique conceptual framework for researchers of information privacy to compare different forms of PCMs in OHCs and distinguish their effects from one another. According to the theory (Bandura, 2001), control can be exerted from three
different levels. Specifically, personal control refers to the influence that one individual’s actions, thoughts or behaviors have over the potential outcomes of a situation in which that individual is involved (Bandura, 2001). Proxy control is exerted by external entities and/or individuals. Via proxy agency, “…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, p.13). Finally, collective control specifies the role of other members of a social system. “Group attainments are the product not only of the shared intentions, knowledge and skills of its members, but also of the interactive, coordinated, and synergistic dynamics of their transactions.” (Bandura, 2001, p. 14). Drawing upon these conceptualizations of control, the present research examines how the three levels of control can be realized through different designs of PCMs.

While the concept of control is central to the notion of privacy (Belanger & Crossler, 2011), not many empirical studies of privacy have measured the degree of control given to individuals or its subsequent effect on the privacy phenomena. As discussed earlier, the influence of privacy assurances, privacy concerns, and motivation to disclose information on risk and trust is similarly inconsistent in presentation and warrants further examination. The inclusion of control constructs represents a unique opportunity for advancing the theoretical development and empirical progress of privacy research.

4.3 Research Model and Hypotheses

Based on the agentic perspective of social cognitive theory (Bandura, 2001) and the privacy literature, the research model is presented in Figure 4.1, along with associated
hypotheses. Control is recognized as an essential construct and consideration in studies of online privacy (Belanger & Crossler, 2011; Margulis, 1977). In this study, it is regarded as a focal construct which is proposed to have the ability to influence an OHC user’s risk perception and trust in the OHC. The three modes of control (personal, proxy, and collective), based on the agentic perspective of social cognitive theory (Bandura 2001), are provided as privacy assurances in the model, and function as information choice and access mechanisms in the context of online health communities (OHC). They serve to clarify the privacy policies that an OHC endorses and information access options from which the OHC members can choose. In the research model, perceived risk and trust are incorporated as important beliefs that influence intention to disclose personal information in an OHC. In addition, global privacy concerns and personal internet interest (PII) are included as relevant individual differences, and age, gender and prior privacy violations are included as control variables based on the existing privacy literature (Belanger and Crossler 2011).

Figure 4.1 - The Research Model
The desire to have personal control over one’s private information is a salient need (Smith and Dinev, 2011), and a first line of defense when sharing information online. If an organization or community can give a certain level of control to its members, each individual member can make the decision of what personal information to share and evaluate the level of risks involved (Xu et al. 2012). In relation to the current research context, an OHC can convey a sense of personal control by providing its community members with the ability to decide which parts of their personal information could be made available to other members in the community. Specifically, members can exercise a relatively high degree of personal control, when an OHC deploys specific privacy assurance mechanisms or interface design elements that allow its members to share as little or as much personal information as they choose. Because OHC members will be able to decide to disclose the amount of personal information that aligns with their own privacy concerns, they are expected to perceive less risk in using the OHC. Therefore, we hypothesize that:

H1a. Higher levels of personal control will result in lower perceived risk in using an OHC.

The mode of proxy control occurs when individuals look to regulatory organizations or other third parties, for assistance in protecting their personal information. IS users may rely on this mode of control, when they do not have complete or sufficient personal control over their personal information. Because exercising personal control is often associated with costs and carries its own burden of responsibility (Bandura, 2001), being able to rely on regulatory agencies to set standards for the sharing and protection of personal information can help reduce personal responsibility and
individual efforts. In an OHC context, healthcare and privacy-related organizations may provide regulatory guidelines or requirements that serve as a proxy for the personal control that users may lack. As an online community adheres to a higher degree of privacy compliance with these regulatory guidelines, its members are expected to perceive less risk in sharing their personal information within the community (Miltgen and Smith, 2015). In other words, when the members of an OHC are made aware that their online community complies with recommended guidelines or requirements from regulatory institutions, the perceived risk from sharing personal information is reduced. As such, we hypothesize:

H1b. Higher levels of proxy control will result in lower perceived risk in using an OHC.

Collective agency provides the third option for maintaining control. This option relies on a “socially coordinative and interdependent effort” (Bandura, 2001, p.1). An online community has shared interests and can work as a collective to further those interests (Bandura, 2000), such as protecting the personal health information of members in an OHC context. That is, within an OHC, individual members can put aside their own interests to work collectively toward a common goal of protecting the personal information of community members. This mode of control can function as an effective defense mechanism to mitigate perceived shared risk. Specifically, it is expected that these collective actions of an OHC can help to alleviate an individual member’s concerns about the severity of exposing others’ information as a result of their own use of OHC as well as the susceptibility of others to information exposure as a result of their own use of OHC (James et al., 2017). As a result, if an OHC user is aware of the community’s
responsibilities with regard to using other member’s information, perceived risk can be reduced. Thus, we hypothesize that:

H1c. Higher levels of collective control will result in lower perceived risk in using an OHC.

A sense of trust is a prerequisite to transacting online and especially when transmitting personal or sensitive information. In order to persuade users to share sensitive information, organizations need to be able to signal their trustworthiness to users (Tang et al., 2008). When an online community provides an explicit mechanism through which members can choose the personal information that they share, the offering of that mechanism, as a privacy assurance, suggests that the community is trustworthy. In other words, the action of providing a web element or artifact that enables members to choose which personal information they are willing to share, suggests that members can trust the community to safeguard their personal information. Privacy research has shown that consumer privacy empowerment (Midha, 2012), an “individual's perception of the extent to which he/she can control the distribution and use of his/her personally identifying information” (p. 200), can have a significant impact on trust. Similarly, OHC members may feel a sense of empowerment regarding their personal information, and their trust in the OHC is increased as a result. Thus, we hypothesize that:

H2a. Higher levels of personal control will result in higher trust in an OHC.

As noted earlier, proxy control in an online privacy context is the reliance on regulatory organizations to safeguard one’s personal information. Past research has indicated that compliance with regulatory standards can impact perceptions of trust in an
online context. Mandatory standards as a privacy protection regime can enable an online vendor to gain a high level of trust from their consumers (Tang et al. 2008). Xu et al. (2012) found that showing an industry-level certification reduced privacy concerns, while Miltgen and Smith (2015) found that regulatory protection increased users’ trust. In the current research context, an OHC can realize proxy control through the disclosure of the regulatory recommendations or requirements that the community follows. By complying with these external guidelines, an OHC can convey to its members that they are concerned about the privacy of members’ personal information and have taken steps to ensure the security of that information. This can in turn enhance members’ perceptions of the trustworthiness of their OHC. Thus, we hypothesize that:

H2b. Higher levels of proxy control will result in higher trust in an OHC.

Collective control, the coordinated efforts of a group with shared interests and common goals (Bandura, 2001), can also increase trust in an online community. Because this mode of collective control is embedded in a social structure and can be regarded as part of a “community responsibility system” (Bandura, 2001, p. 323), it is expected to be a significant source of trust towards a target entity. While the effects of collective control on trust have not been empirically examined in the context of online communities, prior research has indicated that “the shared values of virtual community members have a positive impact on both trust and relationship commitment.” (Wu et. al., 2010, p. 1025). This evidence implies that people care about the collective efforts of other members of a community when it comes to managing other members’ information. If members of an OHC follow agreed upon guidelines in handling personal information, they are expected
to have more confidence that their personal information is secure. Thus, we hypothesize that:

H2c. Higher levels of collective control will result in higher trust in an OHC.

There are a wealth of studies exploring the role of privacy concerns in the IS literature. Some view concerns as an outcome in the privacy phenomena, while others measure concerns as a general, individual difference construct. Specifically, global privacy concerns, taken as a general individual trait, can influence the formation of risk perception and trust. (Malhotra et al., 2004; Midha, 2012; Pramatari & Theotokis, 2009). Individuals with higher levels of privacy concerns tend to perceive greater risk in sharing their personal information (Malhotra et al., 2004). Likewise, OHC members with greater privacy concerns are likely to perceive greater risk in sharing their health information with an OHC community. Thus, we hypothesize that:

H3. Global privacy concerns are positively related to perceived risk in using an OHC.

In addition to general privacy concerns, motivation to use online resources is also a potential determinant of perceived risk in sharing personal information online. Research on online privacy has focused more attention on how extrinsic motivations can encourage information disclosure (Premazzi et al., 2010; Xie et al., 2006), rather than intrinsic or internal motivations for online information disclosure. To extend the extant literature, the present research examines an important intrinsic motivation for online self-disclosure: personal internet interest (PII). According to Dinev and Hart (2006), PII is defined as “cognitive attraction to Internet interactions” (p. 68). It reflects an individual’s
motivation to engage with the online tool or site, and provides a means to capture
general, internal motivations to use the internet (Dinev & Hart, 2006). In this research
model, it is proposed that this intrinsic motivation would likely reduce the perceived
degree of risk of information disclosure in an online community. In an effort to
rationalize the desired behavior, highly motivated individuals often ignore the risk and
potential costs of that behavior (Brewer et al., 2004). In light of this, we expect that in an
OHC, members with higher PII tend to find the perceived risk in sharing their personal
information with the OHC to be lower, as they are likely to rationalize their desired
behavior with risks inherent in such communities. Hence, we hypothesize that:

H4. Personal internet interest is negatively related to the perceived risk of using
an OHC.

Past research has observed that PII can have a positive effect on intention to
disclose information online (Dinev & Hart, 2006). Similar to the relationship between
perceived behavioral control and behavioral intentions in the theory of planned behavior
(TPB) (Ajzen, 1991), motivation to use the internet is proposed to have a direct influence
on intention to disclose information online. There is a close connection between
motivation to behave and intention to behave, and actual behavior (Reychav & Weisberg,
2010). In the context of an OHC, we propose a direct relationship between PII and
intention to behave, i.e., disclose personal information to the OHC. Thus, we hypothesize
that:

H5. Personal internet interest is positively related to intentions to disclose
information to an OHC.
As previously discussed, past research has proposed a number of different causal links between risk and trust, with some depicting risk as an antecedent to trust (Dinev & Hart, 2006), some treating trust as an antecedent to risk (e.g., Jarvenpaa et al., 2000; Malhotra et al., 2004), or other only theorizing one of the two constructs without the presence of the other (e.g., Bansal et al., 2015; Jozani et al., 2020; Midha, 2012). However, a closer examination of the constructs, as defined in a specified context, can offer support for the notion that the risk assessment is a more immediate process, whereas the trust formation process is a more evaluative process involving a more intensive cognitive assessment of the situation at hand (Adjerid et al., 2018; Holmes, 1991; X. Li et al., 2008; Solhaug & Stølen, 2012; Weber et al., 2004). More specifically, the extended privacy calculus (Dinev & Hart, 2006) contends that perceived risk is a negative antecedent of trust in an online context. Further, Tang et al. (2008) defines this construct in a privacy context as “trust is the willingness of one party to be subject to the risks brought by another party’s actions” (p.154). This definition assumes that an individual is aware of the involved risks before making the decision to trust an Internet vendor. In the context of an OHC, we propose that community members are aware of the risks inherent in disclosing one’s personal information, and specifically health information online, and trust is formed with consideration for that risk as well as the privacy assurances offered. Thus, we hypothesize that:

H6. Perceived risk is negatively related to trust in an OHC.

The recognition of perceived risk as an important consideration in online privacy and information disclosure is pervasive across the literature. Evidence of the influence of perceived risk on intention or willingness to provide information, has been documented
in the literature (Malhotra et al., 2004), and even in a personal health information context (Anderson & Agarwal, 2011). Risk has also been examined in a panel data study and found to have a strong negative effect on the use of social media sites (Posey et al., 2010). Thus, we hypothesize that:

H7. Perceived risk is negatively related to intention to disclose information to an OHC.

Finally, the direct effect of trust on the intention to disclose was proposed by the extended privacy calculus (Dinev & Hart, 2006) and later confirmed by Kehr et al. (2015). In the privacy literature, several studies have found specific support for the positive relationship between trust and intention to disclose information (Bansal et al., 2015; Malhotra et al., 2004). Thus, we hypothesize that:

H8. Trust is positively related to intentions to disclose information to an OHC.

Synthesizing our model, several mediating relationships are implicit in the research model shown in Figure 1, including the mediation of general privacy concerns and personal internet interest by perceived risk, and the mediation of the three modes of control by perceived risk and trust. The individual differences are proposed to be mediated by risk based on the previously discussed notion that an elevated risk tends to mitigate the effect of the individual’s interest in the transaction at hand. Each of the three modes of control are operationalized as privacy assurances, and privacy assurances are known to reduce perceived risk and increase trust. Privacy assurances reduce risk by enabling community members to choose the information they wish to disclose or by maximizing control through the additional mechanisms of proxy and collective control.
Trust is increased by privacy assurances, as these visible efforts on the part of the OHC signal to members that the OHC recognizes their privacy concerns and thus is trustworthy.

### 4.4 Study Design

A 2x2x2, between-subjects experimental design was utilized to test the hypotheses, with personal (high/low), proxy (high/low), and collective (high/low) levels of control. Participants were randomly assigned to one of eight treatments. A pre-survey was conducted to measure control variables and other constructs of interest, including age, gender, prior privacy violations, global privacy concerns and personal internet interest. Perceived risk, trust and intention to disclose were measured in a post-survey as the primary outcome variables.

#### 4.4.1 Participants

The target population for this study are adults from the US who use the internet and might visit online communities, and specifically an online health community. Participants were recruited from Amazon Mechanical Turk (MTurk), given that MTurk workers are representative of the target population for this study (Steelman et al., 2014). Each participant received $1.65 for completing the experimental exercise and surveys.

#### 4.4.2 Experimental Process

Participants were recruited and introduced to the research study via Amazon’s Mechanical Turk service (MTurk). In the online recruitment notice, they were given a link to the pre-survey. After responding to the items in the pre-survey, participants were given a scenario in which they were interested in joining a hypothetical web service...
called Aquamarine Health Community. They were then invited to visit the home page of the OCH and read a description of the services offered by this online community. After visiting the landing page, participants were directed to click-through the sign-up process which consisted of a three-step approach specifying the privacy controls used with their personal information. Participants in each of the eight experimental conditions were introduced to the three different forms of control mechanisms, with each of them at a high or low level. After the completion of the simulated sign-up process, the participants were asked to complete a post-survey which contained manipulation check questions and measures of the study’s dependent variables.

4.4.3 Construct Operationalization

The three types of control, or modes of human agency (Bandura, 2001), were operationalized by privacy control descriptions and features provided to participants on the online health community site, as shown in Figures 4.2a-c. The personal high control condition allowed participants to specifically select the individual aspects of their personal information that would be ‘shareable’ across the OHC. The personal low control condition simply stated how their personal information would be used by the OHC, without providing participants with any choices about what information would be shared. The proxy high control condition presented participants with a list of four institutional guidelines with which the OHC complies regarding information privacy. In contrast, the proxy low control condition listed only one entity with which the OHC complies. Lastly, the collective high control condition presented participants with a three-part community code of conduct agreement specifying what constituted proper management of other members’ personal information. Conversely, the low collective control condition simply
showed one statement disclosing that they would have access to other members’ information.
Whenever possible, the scales utilized in the pre and post survey were adapted from the extant literature. All scales are shown in Table 4.1 and were presented as 7-point Likert-type scales, except for the yes/no questions used for prior privacy violations. The global privacy concern scale was adapted from Malhotra et al. (2004). The original Dinev and Hart’s (2006) personal internet interest was adopted. The perceived risk scale from Jarvenpaa and Tractinsky (1999) was adapted and trust was measured based on the scale from Hong and Thong (2013). Finally, the intention to disclose scale was adapted from Bansal et al. (2010).
Table 4.1 - Scales used in Pre and Post Surveys

<table>
<thead>
<tr>
<th>Global Information Privacy Concerns – Adapted from (Malhotra et al., 2004)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>GPC1</td>
<td>1. Compared to others, how worried are you about the way online companies handle your information?</td>
</tr>
<tr>
<td>GPC2</td>
<td>2. How important is it for you to keep your privacy intact from online companies?</td>
</tr>
<tr>
<td>GPC3</td>
<td>3. State your level of agreement with the statement: “In general, I am concerned about threats to my personal online privacy nowadays.”</td>
</tr>
<tr>
<td>GPC4</td>
<td>4. Overall, to what degree are you concerned about the privacy of the information you provide online?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Personal internet interest (Dinev et al., 2006)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>PII1</td>
<td>1. Please indicate your agreement with the question below: “I find that personal interest in the information that I want to obtain from the Internet overrides my concerns of possible risk or vulnerability that I may have regarding my privacy.”</td>
</tr>
<tr>
<td>PII2</td>
<td>2. Please indicate your agreement with the question below: “The greater the interest to obtain a certain information or service from the Internet, the more I tend to suppress my privacy concerns.”</td>
</tr>
<tr>
<td>PII3</td>
<td>3. Please indicate your agreement with the question below: “In general, my need to obtain certain information or services from the Internet is greater than my concern about privacy.”</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Prior Privacy Violations (Bansal et al., 2010) Categorical “yes” vs. “no”</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. To your knowledge, has your private information been compromised in the past?</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Perceived risk (Jarvenpaa &amp; Tractinsky, 1999)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>RISK1</td>
<td>1. It would be risky to give my personal information to Aquamarine Health Community.</td>
</tr>
<tr>
<td>RISK2</td>
<td>2. There would be high potential for loss associated with giving my personal information to Aquamarine Health Community.</td>
</tr>
<tr>
<td>RISK3</td>
<td>3. There would be too much uncertainty associated with giving my personal information to Aquamarine Health Community.</td>
</tr>
<tr>
<td>RISK4</td>
<td>4. Providing Aquamarine Health Community with my personal information would involve many unexpected problems.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Trust (Hong &amp; Thong, 2013)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>TRUST1</td>
<td>1. AquaMarine Health would be trustworthy in handling my personal information.</td>
</tr>
<tr>
<td>TRUST2</td>
<td>2. AquaMarine Health would keep my best interests in mind when dealing with my personal information.</td>
</tr>
<tr>
<td>TRUST3</td>
<td>3. AquaMarine Health would fulfill their promises related to my personal information.</td>
</tr>
<tr>
<td>TRUST4</td>
<td>4. AquaMarine Health would be predictable and consistent regarding the usage of my personal information.</td>
</tr>
</tbody>
</table>
Intention to Disclose – Adapted from (Bansal et al., 2010) 7 pt. Likert-type scale: Extremely unlikely/likely

<table>
<thead>
<tr>
<th>ITD1</th>
<th>1. How likely would be to disclose your own personal medical information to this community?</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITD2</td>
<td>2. How likely would you say you are to actively participate in forums and conversations in this community?</td>
</tr>
<tr>
<td>ITD3</td>
<td>3. How likely are you to provide any sensitive personal information this website requests from you?</td>
</tr>
</tbody>
</table>

Manipulation Check – 7 pt. Likert-type scale.

<table>
<thead>
<tr>
<th>MAN1</th>
<th>1. Aquamarine allows you to control how the personal information in your profile is shared on their website community. (Agree – Disagree)</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAN2</td>
<td>2. Based on the number of different federal guidelines listed by AquaMarine, how would you assess the strength of AquaMarine's compliance with relevant privacy guidelines. (Very Weak – Very Strong)</td>
</tr>
<tr>
<td>MAN3</td>
<td>3. Aquamarine’s community code of conduct provides specific rules stating what members cannot do with other community members' personal information. (Agree – Disagree)</td>
</tr>
</tbody>
</table>

4.5 Results

A total of 228 participants completed the study and took slightly less than 11 minutes on average. As recommended by Wessling et. al. (2017) when working with data collected from Mturk, attention check questions were included in the pre and post surveys, and other procedures were followed to clean the data. As a result, 26 observations were eliminated from the analysis for either having been completed the survey in under 4 minutes or having failed to answer an attention check question correctly. The following data analysis includes 202 participants’ data. A table of descriptive statistics for all measured variables, by treatment, is detailed in Table 4.2.
Table 4.2 - Descriptive Statistics - Means by Treatment

<table>
<thead>
<tr>
<th></th>
<th>Personal</th>
<th></th>
<th></th>
<th>Proxy</th>
<th></th>
<th></th>
<th>Collective</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>High</td>
<td>Low</td>
<td>High</td>
<td>Low</td>
<td>High</td>
<td>Low</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>N</td>
<td>24</td>
<td>28</td>
<td>26</td>
<td>21</td>
<td>26</td>
<td>27</td>
<td>24</td>
<td>26</td>
<td>26</td>
</tr>
<tr>
<td>Trust</td>
<td>5.177</td>
<td>5.009</td>
<td>4.702</td>
<td>4.643</td>
<td>4.317</td>
<td>4.185</td>
<td>3.927</td>
<td>3.625</td>
<td></td>
</tr>
<tr>
<td>Intention to Disclose</td>
<td>3.875</td>
<td>4.071</td>
<td>3.359</td>
<td>3.571</td>
<td>3.231</td>
<td>3.284</td>
<td>2.583</td>
<td>2.923</td>
<td></td>
</tr>
</tbody>
</table>

4.5.1 Manipulation checks

Manipulation check questions were included in the post-survey, as shown in Table 4.1, to determine whether the experimental manipulations were successful. Based on Perdue and Summers (1986), an analysis was conducted to ensure that each treatment manipulated the desired construct (levels of control) without confounding other treatments. As shown in Table 4.3, the treatment manipulations were successful for the desired construct (3 modes of control), without confounding the other manipulations. This indicates that while the changes implemented to alter the levels of each of the three modes of control were perceived by the participants as such, they had little effect on perceptions of the other modes of control.

Table 4.3 – Manipulation Check Analysis

<table>
<thead>
<tr>
<th></th>
<th>Personal Control</th>
<th></th>
<th>Proxy Control</th>
<th></th>
<th>Collective Control</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>p-value</td>
<td>F</td>
<td>p-value</td>
<td>F</td>
<td>p-value</td>
<td>F</td>
</tr>
<tr>
<td>Item1 Personal</td>
<td>&lt;.001*</td>
<td>222.276</td>
<td>.045</td>
<td>4.088</td>
<td>.564</td>
<td>.333</td>
</tr>
<tr>
<td>Item 2 Proxy</td>
<td>.491</td>
<td>.476</td>
<td>&lt;.001*</td>
<td>101.481</td>
<td>.634</td>
<td>.227</td>
</tr>
<tr>
<td>Item 3 Collective</td>
<td>.728</td>
<td>.121</td>
<td>.858</td>
<td>.032</td>
<td>&lt;.001*</td>
<td>128.577</td>
</tr>
</tbody>
</table>

*p-value < 0.001
4.5.2 Measurement Validity and Reliability

Reliability analysis was performed using Cronbach’s alpha and an exploratory factor analysis (EFA) was conducted using Varimax rotation with Principal Components Analysis. Both procedures were performed via IBM SPSS 28. Table 4.4 provides the reliability analysis results, with all reliabilities exceeding .90 suggesting strong reliability (Cortina, 1993; Nunnally, 1978). Support for the convergent and discriminant validity of the constructs is provided in Table 4.4, where the average variance extracted (AVE) scores are all above 0.5, suggesting good convergent validity (Podsakoff et al., 2003), and the square root of the AVE scores for all the constructs are higher than the correlation values, satisfying discriminant validity guidelines (Mackenzie et al., 2011). The EFA results (Table 4.5) also show good convergent and discriminant validity\(^2\), with items loading properly onto their factors with factor loadings above 0.79 and all cross loadings are at or under 0.3, meeting the standard for discriminant validity suggested by Kordzadeh and Warren (2017) of 0.7 or above for loadings and 0.3 or less for cross loading scores.

Table 4.4 - Reliability, Correlations, and Average Variance Extracted

<table>
<thead>
<tr>
<th></th>
<th>Alpha</th>
<th>CR</th>
<th>AVE</th>
<th>PII</th>
<th>GPC</th>
<th>Trust</th>
<th>Risk</th>
<th>ITD</th>
</tr>
</thead>
<tbody>
<tr>
<td>PII</td>
<td>.906</td>
<td>.927</td>
<td>0.808</td>
<td>.899</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GPC</td>
<td>.906</td>
<td>.912</td>
<td>0.723</td>
<td>-.153*</td>
<td>.850</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trust</td>
<td>.955</td>
<td>.940</td>
<td>0.796</td>
<td>.316**</td>
<td>-.153*</td>
<td>0.892</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk</td>
<td>.955</td>
<td>.917</td>
<td>0.734</td>
<td>-.209**</td>
<td>.462**</td>
<td>-.543**</td>
<td>0.857</td>
<td></td>
</tr>
<tr>
<td>Intention to Disclose</td>
<td>.918</td>
<td>.787</td>
<td>0.551</td>
<td>.348**</td>
<td>-.154*</td>
<td>.681**</td>
<td>-.554**</td>
<td>0.743</td>
</tr>
</tbody>
</table>

\(^{**} p < 0.01, * p< 0.05. Square Root of AVE on the diagonal\)

\(^2\) During pilot tests, one item from the Global Privacy Concern scale showed poor convergent and discriminant validity. This item read “All things considered, the Internet would cause serious privacy problems.” Upon further analysis, this item is the only one that reflects on the nature of the Internet without any reference to the participant’s privacy. This item was dropped from the study.
Table 4.5 - Factor Loadings from Exploratory Factor Analysis

<table>
<thead>
<tr>
<th>Component</th>
<th>GPC</th>
<th>PII</th>
<th>Trust</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>GPC1</td>
<td>-0.057</td>
<td>0.245</td>
<td>0.791</td>
<td>0.043</td>
</tr>
<tr>
<td>GPC2</td>
<td>-0.027</td>
<td>0.114</td>
<td>0.841</td>
<td>-0.150</td>
</tr>
<tr>
<td>GPC3</td>
<td>-0.019</td>
<td>0.199</td>
<td>0.876</td>
<td>-0.051</td>
</tr>
<tr>
<td>GPC4</td>
<td>-0.052</td>
<td>0.207</td>
<td>0.889</td>
<td>-0.063</td>
</tr>
<tr>
<td>PII1</td>
<td>0.161</td>
<td>-0.029</td>
<td>-0.075</td>
<td>0.894</td>
</tr>
<tr>
<td>PII2</td>
<td>0.126</td>
<td>-0.090</td>
<td>-0.033</td>
<td>0.899</td>
</tr>
<tr>
<td>PII3</td>
<td>0.137</td>
<td>-0.086</td>
<td>-0.082</td>
<td>0.904</td>
</tr>
<tr>
<td>TRUST1</td>
<td>0.911</td>
<td>-0.254</td>
<td>-0.034</td>
<td>0.176</td>
</tr>
<tr>
<td>TRUST2</td>
<td>0.911</td>
<td>-0.209</td>
<td>0.015</td>
<td>0.080</td>
</tr>
<tr>
<td>TRUST3</td>
<td>0.892</td>
<td>-0.249</td>
<td>-0.089</td>
<td>0.142</td>
</tr>
<tr>
<td>TRUST4</td>
<td>0.854</td>
<td>-0.281</td>
<td>-0.064</td>
<td>0.165</td>
</tr>
<tr>
<td>RISK1</td>
<td>-0.298</td>
<td>0.839</td>
<td>0.247</td>
<td>-0.097</td>
</tr>
<tr>
<td>RISK2</td>
<td>-0.225</td>
<td>0.863</td>
<td>0.265</td>
<td>-0.089</td>
</tr>
<tr>
<td>RISK3</td>
<td>-0.302</td>
<td>0.863</td>
<td>0.204</td>
<td>-0.088</td>
</tr>
<tr>
<td>RISK4</td>
<td>-0.260</td>
<td>0.862</td>
<td>0.218</td>
<td>-0.023</td>
</tr>
</tbody>
</table>

An additional assessment of convergent and discriminant validity was conducted by running a confirmatory factor analysis (CFA) using MPlus 7 for all the latent variables measured, including PII, perceived risk, trust, and intention to disclose. Fit statistics for the CFA model (CFI:0.973; RMSEA: 0.061; SRMR: 0.035) all exceeded recommended thresholds (Kline & Santor, 2016), suggesting good fit of the measurement model, as well as strong convergent and discriminant validity.

### 4.6 Analysis and Results

A multivariate analysis of covariance (MANCOVA) test was conducted using SPSS 28 to test hypotheses H1-H5. Table 4.6 summarizes the study results. Several control variables included in the model had significant effects. Age had a significant effect on perceived risk, with older participants reporting higher levels of perceived risk (p-value .020). Gender also had a significant effect on perceived risk with women
reporting higher levels of perceived risk than men (p-value .041). Trust and intention to disclose did not differ by age or gender. Prior privacy violations did not affect perceived trust or intention to disclose but did have a negative relationship with intention to disclose (p-value .035).

The personal control treatment presents a significant effect on perceived risk and trust, with participants in the high personal control treatment reporting lower risk (4.05\text{high}, 4.91\text{low}, p-value <.001) and higher trust (4.89\text{high}, 4.02\text{low}, p-value <.001) than those in the low personal control treatment, supporting H1a and H2a. The proxy control treatment shows an effect on trust (4.66\text{high}, 4.21\text{low}, p-value =.026), but not perceived risk, supporting H3b. The third treatment, collective control, shows an effect on perceived risk (4.29\text{high}, 4.67\text{low}, p-value =.011), but not on trust, supporting H1a. Considering all three treatments of control, perceived risk ranged from 3.95 to 5.11, and trust ranged from 5.18 to 3.63, for high levels of personal, proxy and collective control and for low levels of personal, proxy and collective control, respectively. The relationship between global privacy concerns and perceived risk was supported (H3), as were the relationships between personal internet interest and perceived risk (H4) and with intention to disclose (H5). The study findings for H6-8 and an assessment of the proposed mediation relationships are provided in the next subsection.

Table 4.6 - MANCOVA results

<table>
<thead>
<tr>
<th></th>
<th>Dependent Variables</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Perceived Risk</td>
<td>Perceived Trust</td>
<td>Intention to Disclose</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>F</td>
<td>p-value</td>
<td>F</td>
<td>p-value</td>
<td>F</td>
</tr>
<tr>
<td>Age</td>
<td>5.53</td>
<td>.02</td>
<td>3.493</td>
<td>.063</td>
<td>1.071</td>
</tr>
<tr>
<td>Gender</td>
<td>4.215</td>
<td>.041</td>
<td>1.462</td>
<td>.228</td>
<td>.874</td>
</tr>
<tr>
<td>PII</td>
<td>11.106</td>
<td>.001</td>
<td>15.705</td>
<td>&lt;.001</td>
<td>24.305</td>
</tr>
</tbody>
</table>
4.6.1 Structural Regression Model

A structural regression model was run using MPlus 7, to test H6-H8 and to confirm some of the MANCOVA results. Alternative research model configurations were also run to assess full vs. partial mediation effects. The results are presented in Figure 4.2. Fit statistics for the proposed model are presented in Table 7 and suggest good fit with all indices exceeding recommended values (Kline & Santor, 2016).

Table 4.7 - Structural Regression Model Fit Statistics

<table>
<thead>
<tr>
<th>Test</th>
<th>Value</th>
<th>Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normed Chi Square</td>
<td>1.97</td>
<td>&lt; 2 is ideal; &lt; 3 is acceptable</td>
</tr>
<tr>
<td>CFI</td>
<td>0.968</td>
<td>Above &gt;.9 acceptable;</td>
</tr>
<tr>
<td>RMSEA</td>
<td>0.065</td>
<td>Between .05 and .08 is adequate</td>
</tr>
<tr>
<td>SRMR</td>
<td>0.068</td>
<td>&gt; .1 indicates poor fit</td>
</tr>
</tbody>
</table>
The hypothesized relationships are supported with a significant path between perceived risk and trust (H6: -.565, p-value<.001), and significant paths between perceived risk and intention to disclose (H7: -.120, p-value=.047), and between trust and intention to disclose (H8: .619, p-value<.001). Further, the results indicate empirical support for the relationships between global privacy concerns and perceived risk (H3: .458, p-value<.001); personal internet interest and perceived risk (H4: -.162, p-value=.010); and personal internet interest and intention to disclose (H5: .201, p-value<.001), confirming the MANCOVA results. A summary of the results is provided in Table 4.8.

Table 4.8 - Hypotheses Results

<table>
<thead>
<tr>
<th>Hypotheses</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>H1 Higher levels of (a) personal, (b) proxy, and (c) collective control will result in lower perceived risk in using an OHC.</td>
<td>H1a and H1c supported</td>
</tr>
<tr>
<td>H2 Higher levels of (a) personal, (b) proxy, and (c) collective control will result in higher trust in an OHC.</td>
<td>H2a and H2b supported</td>
</tr>
<tr>
<td>H3 General privacy concerns are positively related to perceived risk of using an OHC.</td>
<td>Yes</td>
</tr>
<tr>
<td>H4 Personal internet interest is negatively related to perceived risk of using an OHC.</td>
<td>Yes</td>
</tr>
<tr>
<td>H5 Personal internet interest is positively related to intentions to disclose information to an OHC.</td>
<td>Yes</td>
</tr>
<tr>
<td>H6 Perceived risk is negatively related to trust in an OHC.</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Given the mediation proposed in the research model, with GPC and PII not having a direct effect on trust, two alternative models were considered as shown in Figure 4.3. Model 2 is a fully mediated model with no direct effects from PII or perceived risk to intentions to disclose. Model 3 is a no mediation model in which GPC and PII having direct effects on trust, instead of risk mediating these effects. The fit statistics for these models are shown in Table 4.9, along with the fit statistics from the proposed model. While fit statistics for all three models are acceptable, the results suggest that the proposed Model #1 (chosen for this study) provides the best fit.

<table>
<thead>
<tr>
<th>Hypotheses</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>H7 Perceived risk is negatively related to intentions to disclose information to an OHC.</td>
<td>Yes</td>
</tr>
<tr>
<td>H8 Trust is positively related to intentions to disclose information to an OHC.</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Model</th>
<th>Normed Chi Square</th>
<th>CFI</th>
<th>RMSEA</th>
<th>SRMR</th>
<th>Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model #1 (proposed)</td>
<td>1.8</td>
<td>0.959</td>
<td>0.059</td>
<td>0.048</td>
<td>&lt; 2 is ideal; &lt; 3 is acceptable</td>
</tr>
<tr>
<td>Model #2</td>
<td>2.08</td>
<td>0.963</td>
<td>0.069</td>
<td>0.084</td>
<td>&gt; .95 indicates good fit</td>
</tr>
<tr>
<td>Model #3</td>
<td>2.45</td>
<td>0.952</td>
<td>0.08</td>
<td>0.125</td>
<td>&gt; .05 &amp; &lt; .08 is adequate</td>
</tr>
</tbody>
</table>

Figure 4.3 - Alternative models considered

Table 4.9 - Alternative Models and Fit Statistics
4.7 Discussion and Contributions

This research examined the effects of three modes of control, general privacy concerns and personal internet interest on perceived risk, trust, and intention to disclose in an online setting. Most of the hypotheses were supported and are discussed at length below. The control variables of age and gender were found to have the anticipated effects on perceived risk, with older participants and women perceiving higher risk, while the measure of prior privacy violations was negatively related to intentions to disclose information. These findings for age and gender support a conceptualization of perceived risk as an immediate assessment and process in the context of joining a new online health community, which would be more susceptible to individual differences. At the same time, this supports the notion that trust is a more extensive, evaluative process with stronger influence from privacy assurances and a more elaborate cognitive process when compared to risk perception. The findings for prior privacy violations suggest that this individual difference overrides perceived risk and trust, and deters users from disclosing personal information regardless of any privacy assurances that are present.

Results for the three modes of control suggest that privacy assurances for personal control have a stronger influence on perceived risk and trust, compared to the other modes of control. These findings are not surprising, as individual control provides direct oversight over whether personal information is shared, or not shared. Proxy and collective control are indirect in that these forms of control are only relevant for personal information that has been shared, and are applicable in general terms over all information shared within a community, not just one member’s information. Bandura notes that part of the “price of proxy agency is a vulnerable security that rests on the competence,
power, and favors of others” (2001, p.13), and the same applies to collective control.

When relying on proxy and collective control, one is inherently relying on others, which is a more vulnerable situation than relying on oneself. In our study, greater personal control influenced both perceived risk and trust, suggesting that the presence of privacy assurances for personal control can be used to encourage information disclosure.

Perceived risk was lower and trust was higher when stronger privacy assurances were provided for personal control, giving community members control over what personal information would be shared in the OHC.

Proxy control, as operationalized through privacy assurances, influenced trust but did not influence perceived risk. The privacy assurances for proxy control provided evidence of greater regulatory oversight (i.e., compliance with four recommended guidelines) when proxy control was high, and less oversight when proxy control was low (i.e., compliance with one recommended guideline). Greater levels of compliance seemed to make the OHC appear more trustworthy, but did not influence perceived risk, likely because most community members are less familiar with these guidelines and how these guidelines can actually protect their personal information. In other words, community members are unlikely to be familiar with these external, regulatory institutions and how these institutions’ guidelines protect their privacy, thus their perceived risk will be less affected by this form of control. This explanation is supported by existing research on privacy assurances which found that the presence of privacy seals tended to be effective only when the system users understood the intended meaning of privacy seals (Lowry et al., 2012). As an evaluative process, trust was higher for participants who experienced high proxy control, as the OHC had taken actions to protect members’ personal
information. Since the OHC exhibited trustworthy behavior, it was rewarded with higher trust.

Last, the privacy assurances for collective control influence perceived risk but not trust. This interesting finding suggests that the privacy assurance used to operationalize collective control, a stronger or weaker community code of conduct, reduced perceived risk but did not build trust. In other words, a community code of conduct that must be followed by all members, did not influence members’ trust in the OHC as a collective entity. These findings may reflect the different referent objects, community members as compared to the OHC itself.

In assessing the individual differences that were hypothesized, general privacy concerns influenced perceived risk but not trust, while personal internet interest influenced both perceived risk and trust. The conceptual differences in perceived risk and trust may explain these findings. General privacy concerns (GPC), an individual difference that reflects an individual’s accumulation of prior privacy concerns, is known to positively affect individual’s perceived risk (Kehr et al., 2015). Concerns and perceived risk are highly related (Miltgen & Smith, 2015). Privacy concerns and trust were expected to be negatively related. It is possible that privacy assurances dominated the trust formation process, and thus GPC had little effect on trust. Personal internet interest (PII) reflects a community member’s general motivation to use the internet, and thus potentially a member’s motivation to use an OHC. PII had significant effects on perceived risk and trust, suggesting that motivation has a powerful effect not just on behavior but also on beliefs known to influence behavior.
The hypothesized relationships between perceived risk, trust, and intention to disclose information were all supported, as was the direct positive relationship between PII and intention to disclose. Further, the mediation tests conducted supported the sequence of relationships proposed, as a fully mediated model and unmediated model all showed lower fit than the proposed model. One of the objectives of this study was to explore the relationship between risk and trust. Although these constructs are commonly used in the privacy literature, the causal direction between these two constructs hasn’t found consensus. Our study conceptualized perceived risk as a brief process in which an individual quickly gathers contextual cues and evaluates the risks in any given situation based on their own PII and GPC. The trust formation process is a more involved cognitive evaluation which includes the perception of risk. In fact, one of the strongest significant predictive relationships in our model is that of risk on trust. Research on PII has primarily studied the relationship with intention to disclose information, which is also confirmed in the current study. In addition, the relationship between PII and perceived risk and trust is supported, and PII is shown to be a powerful determinant of an individual’s intention to disclose information through more than one causal path. Further, our study has shown that PII has the capacity to regulate or even overcome other negative influences such as privacy concerns.

Contributions of this research include both theoretical and practical implications. From a theoretical perspective, the conceptual development of the three modes of control (personal, proxy and collective), based on the agentic perspective of social cognitive theory, in an online community context, provides a novel, theoretical approach for integrating control, privacy concerns, and information disclosure. While IS research has
acknowledged the strong relationship between control and privacy concerns, many studies have not incorporated control or have considered it only as a dimension of privacy concerns. Only one other privacy study has incorporated control as a separate construct with different modes or forms of control (Xu et al., 2012), and no other study has conceptualized both proxy and collective control. Further, privacy scholars have noted the absence of research on group-level privacy and have called for future empirical studies that target these group levels of analysis (H. J. Smith et al., 2011).

Theoretical contributions also include the proposed and supported causal and mediated relationships with perceived risk, trust and intention to disclose. Perceived risk and trust were measured in a context-specific manner after participants were exposed to the experimental website and the privacy assurance treatments. We conceptualized perceived risk as an initial and more immediate assessment of the perceived risks inherent in an information disclosure context, which would be influenced by the individual differences of PII and GPC, which was supported. Perceived risk was a determinant of trust and both perceived risk and trust were determinants of intention to disclose personal information. The three modes of control were proposed to reduce perceived risk and increase trust in the OHC and these relationships were largely supported. The mediated model did not support a direct effect of control on intention to disclose.

Significant practical implications are provided by the operationalization of control through privacy assurances. Our theory-driven work on privacy assurances, with privacy assurance mechanisms developed for all three modes of control in an online community context, provides a great exemplar for how websites and online communities can be
designed to showcase and deliver these important forms of control to users. Further, the parsimonious research model incorporates highly relevant constructs that are easily measured and contributes to a high level of explained variance in outcome variables.

4.8 Conclusion and Limitations

As with all research there are limitations that should be acknowledged. An experimental scenario with an online health community was used as the context for this study. While every effort was made to develop a realistic website, the context was experimental, and the participants did not actually have health concerns or seek out an OHC for personal reasons. The results would be more meaningful and potentially have larger effects were an actual OHC used in the study.

In this research, a theoretical model of control and privacy concerns based on the agentic perspective of social cognitive theory was developed and tested in an OHC context. Privacy assurances for personal, proxy and collective control modes were operationalized and tested in an experimental context. Relevant individual difference variables, global privacy concerns and personal internet interest, were incorporated and provided strong explanatory power for understanding both concerns and motivation to disclose personal information in an OHC context. A comprehensive set of outcome variables were examined, including perceived risk, trust, and intention to disclose personal information, and substantial variance in these constructs was explained. The model and results provide a foundation for future privacy research on control, and particularly different forms or levels of control. Research on privacy assurances was also advanced based on the successful operationalization of three control mechanisms.
CHAPTER 5

IMPLICATIONS, FUTURE RESEARCH AND CONCLUSION

5.1 Summary of Chapters

To examine privacy concerns in online settings and with online health communities specifically, the following broad research questions were addressed in this dissertation:

1. How widely has the concept of privacy been studied in the online health community setting and in online settings in general?

2. Which are the most prevalent antecedents, privacy-related constructs, and outcomes in the online privacy-related IS research?

3. What knowledge gaps exist in the literature that may further the understanding of privacy in online health communities?

4. How do control, privacy assurances and information sensitivity influence specific forms of privacy concerns and common outcomes?

5. How do different types of control affect the impact of privacy concerns on the formation of trust, risk and intention to disclose information?

5.2 Conceptual and Theoretical Implications

The roadmap presented by this dissertation, starts by performing an assessment of the state of the privacy literature in Information Systems (IS). Potential areas for further study and development are identified and include:
First, limited empirical investigation of the role of control and how it impacts privacy concerns, risk, and trust are found in the literature. Second, the interplay between control, information sensitivity, and privacy assurances has not been studied together in the privacy phenomena. Third, while personality is used in the privacy literature, no consensus exist in the overall effect of NEO personality traits on the privacy phenomena and an opposing effect of agreeableness is shown. Fourth, the relational path between trust and risk (both highly used constructs in the privacy literature in IS) sees some conflicting findings. Finally, information sensitivity, while commonly accepted as an important construct in privacy, has not been measured in a comparative, experimental health-related setting. Chapter 3 introduces the role of privacy assurances and information sensitivity (context) along with control, as potential antecedents to the notorious privacy calculus model which includes the prominent privacy concerns construct. The study is an experimental analysis of the combined effect of these manipulated variables in an online setting for two fictitious vendors. The results of this study provide insight into the important, yet neglected, role of control in the privacy phenomena demonstrating its significant impact on all hypothesized relationships. Information sensitivity is confirmed to have a specific effect on the participants’ privacy concerns while privacy assurances are shown to influence the trust that users feel for the company/vendor. The combined effect of control and privacy assurances in the individual formation of trust as a specific attitude towards the web service is also unveiled by this study. In sum, all the experiment treatment variables of the study (control, privacy assurances, and information sensitivity) are found to have an effect on different parts of the privacy calculus model. This serves as the background for a number of theoretical
implications which expand the state of the literature in privacy and identify new venues for further research.

In chapter 4, a richer conceptualization of control is adopted as a central construct. Three distinct levels of control are manipulated in an experimental online setting where privacy concerns, are conceptualized as an individual trait-like (context-independent) characteristic of the participants/users. The resulting effects on the formation of trust, risk and intention to disclose information provide a strong contribution as this study is the first to operationalize the collective level of control and include three levels of control in an empirical study. Such specific-interest social networks have gained recent popularity and this study sheds light onto the privacy phenomena within them. The results of this study provide insight into the importance of one of the most important constructs in the study of privacy: control. It also informs practitioners of the potential benefits of adopting a more elaborate conceptualization of control as well as the use of privacy assurances conveyed as an IT artifact. This study applies a novel and interesting theoretical background adopted from the psychology field in the study of privacy and explores the complementary role of different levels of control in privacy. Researchers and practitioners may employ this knowledge to develop new scenarios and real-life applications for the utilization of control and privacy assurances as means to maximize self-disclosure among online users.

Taken together, chapters 3 and 4 examine and test a comprehensive collection of antecedents to privacy concerns, include experimental treatments, individual traits, and prior privacy experiences. Further, chapter 3 tests an existing theoretically driven model of privacy, the privacy calculus in the novel contexts of online health communities. As
demonstrated in Chapters 2 and 3 of this dissertation, the information sensitivity of the context has an important effect in the development and formation of privacy-related concerns for users. The empirical studies introduced in this dissertation taken together, provide a quantifiable analysis of the importance of such setting or context.

Collectively, the literature review along with the empirical studies expand the possibilities of further research in privacy. They also provide a quantifiable understanding of how websites may maximize the individuals’ intention to provide information, as well as the importance of customizing online products and services to the specific needs of the users. Key privacy-related constructs such as trust, risk and control are studied in experimental environments to better understand the causal phenomena underlying privacy. In general, this dissertation proposal seeks to improve the online users’ participation in, and adoption of modern online services resulting in the maximization of benefits for both users and organizations transacting over the internet.

5.3 Practical Implications

Several implications for the practitioner are unveiled by this dissertation. Firstly, the online artifact can present control tools which are demonstrated to have a significant effect in the users’ intention to disclose information and participation in online communities. Second, privacy assurances as characteristics of a website are shown to have influence over the customers’ trust and practitioners may use these to enhance their customers’ trust towards the site. Third, the inclusion of control tools into online communities is also an efficient way to ensure participation and disclosure in these communities. Fourth, evidence for the combined effect of control and privacy assurances on the individual degree of trust is provided which can be useful in settings where the
exchanged information may be seen as inherently sensitive. Finally, the concluding chapter of this dissertation discusses several future research directions that build on this work and layout a path for expanding the knowledge of privacy in information systems.

5.4 Future Research

The work presented in this dissertation manuscript paves the road to a series of future potential research extensions. First, research on privacy and related constructs such as personal internet interest is needed to examine changing perceptions and influence as our online lives have undertaken dramatic changes since privacy concepts were first introduced. For example, four out of six hypothesized relationships of the model tested in Chapter 3 were supported as anticipated, but two were not. One potential venue to address this is conduct a time series meta-analysis to examine how privacy-related perceptions and outcomes have changed over time. Alternatively, different paths in the causal model might be considered based on context and changing privacy perceptions.

Second, further research on privacy assurances and possible moderating effects from control and information sensitivity are warranted, based on the findings of Chapter 3. A research design with different forms of privacy assurance, with central and peripheral cues, might shed more light on how privacy assurances are processed by users, and how these assurances can be strengthened. A more comprehensive examination of information sensitivity might also be fruitful for understanding when individual’s are less likely to disclose information. Rather than just high or low levels of information sensitivity, the context of sharing information could be relevant. For example, online communities may result in different levels of sensitivity than online services or products offered in an arms-length transaction, regardless of the type of information shared. In general, privacy
studies in special-interest communities and/or specialized social networks present potential for the understanding of privacy, its importance and potentially, its change and evolution with the adoption of new information technologies.
BIBLIOGRAPHY


Boonstra, A., & Broekhuis, M. (2010). *Barriers to the acceptance of electronic medical records by physicians from systematic review to taxonomy and interventions.*


Frost, J. H., & Massagli, M. P. (2008). Social uses of personal health information within PatientsLikeMe, an online patient community: What can happen when patients have access to one another’s data. *Journal of Medical Internet Research, 10*(3). https://doi.org/10.2196/jmir.1053


https://doi.org/10.1002/dir.20009

https://doi.org/http://dx.doi.org/10.1057/ejis.2013.17

https://doi.org/10.1016/j.im.2015.06.006


https://doi.org/10.1287/isre.1040.0015


https://doi.org/10.1016/S0065-2601(08)60214-2


Solhaug, B., & Stolen, K. (2012). *Uncertainty, Subjectivity, Trust and Risk: How It All Fits together.* https://doi.org/10.1007/978-3-642-29963-6_1


