2013

Cloud Privacy Audit Framework: A Value-Based Design

David Coss
Virginia Commonwealth University

Follow this and additional works at: https://scholarscompass.vcu.edu/etd

Part of the Technology and Innovation Commons

© The Author

Downloaded from
https://scholarscompass.vcu.edu/etd/3106

This Dissertation is brought to you for free and open access by the Graduate School at VCU Scholars Compass. It has been accepted for inclusion in Theses and Dissertations by an authorized administrator of VCU Scholars Compass. For more information, please contact libcompass@vcu.edu.
CLOUD PRIVACY AUDIT FRAMEWORK: A VALUE-BASED DESIGN

A dissertation proposal submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Business at Virginia Commonwealth University

by

DAVID LEWIS COSS

Master of Business Administration
University of Nevada, Las Vegas, NV 2002
Bachelor of Science in Hotel Administration
University of Nevada, Las Vegas, NV 1998

Director: Dr. Gurpreet Dhillon
Department of Information Systems

Virginia Commonwealth University
Richmond, Virginia
February 2013
Acknowledgement

I would like to first, thank my fiancé, Kathy, for her unwavering support, which got me through what seemed at times an endless pursuit towards the completion of this dissertation. She has kept me grounded and focused as to what is truly important in this life, that of unconditional love. Thank you, Kathy. I love you very much.

This dissertation would not have been possible without the guidance and support of my dissertation chair, Dr. Dhillon. For the last fourteen years, he has been a professor, friend and mentor to me. Eleven years ago when I was finishing my masters with Dr. Dhillon at University of Nevada, Las Vegas, as the gifted professor we all know him to be, he planted a “seed” or “idea” for me to pursue my PhD. Years later, when I was ready to come back to academia, he was waiting with a smile like he knew all along that I would be going down this path. He has been a constant guide in my academic and intellectual journey always challenging and encouraging me along the way. It is not unknown that I sometimes take the long way around things in life, and he has always been there to ever patiently to nudge me back in the right direction when needed. He truly has a gift of knowing when to wear the hat of a friend, professor, mentor, or dissertation chair, and for this I will be forever grateful to him.

I would also like to thank all my committee members, Doctors George Kasper, Richard Redmond, Matthew Rutherford, Manoj Thomas for their support and encouragement throughout this dissertation process. I also would like to thank Doctors
Allen Lee, Roland Weistroffer and Peter Aiken for your guidance and support through the seminar phase of the PhD program, they all had a positive influence on my scholarly development. I would also like to thank Doctors John Moore, Cheryl Mitchem, Dean Mirta Martin and Merri Incitti at Virginia State University for providing me with the necessary motivation, advice and the time to finish this dissertation and for hiring me as a faculty member at VSU.

I made several friends in the graduate school who not only provided unique insights into my scholarly activities but also extended constant encouragement, and support. Thanks to Sushma Mirshra, Mark Harris, Mike Lapke, Basil Hamdan, Fari Nasution, Moe Hawamdeh, Yurita Yakimin Abdul Talib, Ifeoma Udeh, Gray Loftin, Bernie Frankas, Dan Han, Goran Gustavsson, Robert Dahlberg for your friendship.

Lastly I want to acknowledge my late Parents. From my mother, Ann Catherine Coss who past early in my life, I learned to appreciate life itself. From my father, Francis Serial Coss, I learned the importance of a having a strong work ethic and values. I also adopted his desire to be constantly striving to improve oneself. When I was a boy he would say that I was going to be the Doctor in the family, I can now proudly say that I am a Doctor, and I dedicate this work to him.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>TABLE OF CONTENTS</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABSTRACT</td>
<td>viii</td>
</tr>
<tr>
<td>CHAPTER</td>
<td></td>
</tr>
<tr>
<td>1 INTRODUCTION</td>
<td></td>
</tr>
<tr>
<td>1.1 Introduction</td>
<td>11</td>
</tr>
<tr>
<td>1.2 Problem Domain: The Relationship Between Technology and Privacy</td>
<td>13</td>
</tr>
<tr>
<td>1.3 Concepts and Definitions</td>
<td>15</td>
</tr>
<tr>
<td>1.4 Research Argument and Proposed Research Questions</td>
<td>18</td>
</tr>
<tr>
<td>1.5 Dissertation Structure</td>
<td>19</td>
</tr>
<tr>
<td>2 LITERATURE REVIEW</td>
<td></td>
</tr>
<tr>
<td>2.1 Introduction</td>
<td>22</td>
</tr>
<tr>
<td>2.2 Values Literature Review</td>
<td>23</td>
</tr>
<tr>
<td>2.2.1 Individual Level Perspective of Values</td>
<td>24</td>
</tr>
<tr>
<td>2.2.2 Organizational Level Perspective of Values</td>
<td>27</td>
</tr>
<tr>
<td>2.2.3 Societal Level Perspective of Values</td>
<td>31</td>
</tr>
<tr>
<td>2.2.4 Theory of Values as a Theoretical Foundation</td>
<td>34</td>
</tr>
<tr>
<td>2.3 Privacy Literature Review</td>
<td>36</td>
</tr>
<tr>
<td>2.3.1 Privacy Debate</td>
<td>37</td>
</tr>
<tr>
<td>2.3.2 Privacy Ethics and Society</td>
<td>39</td>
</tr>
<tr>
<td>2.3.3 Information Privacy</td>
<td>40</td>
</tr>
<tr>
<td>2.3.4 Online Privacy</td>
<td>41</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>2.3.5 Location Based Privacy</td>
<td>45</td>
</tr>
<tr>
<td>2.3.6 Cloud Privacy</td>
<td>46</td>
</tr>
<tr>
<td>2.4 Discussion</td>
<td>50</td>
</tr>
<tr>
<td>2.5 Conclusion</td>
<td>51</td>
</tr>
<tr>
<td>3 THEORY and RESEARCH DESIGN</td>
<td></td>
</tr>
<tr>
<td>3.1 Introduction</td>
<td>53</td>
</tr>
<tr>
<td>3.2 Theoretical Concepts</td>
<td>54</td>
</tr>
<tr>
<td>3.2.1 Value Focused Thinking</td>
<td>55</td>
</tr>
<tr>
<td>3.2.2 Design Science Concepts</td>
<td>58</td>
</tr>
<tr>
<td>3.3 Research Methodology and Design</td>
<td>62</td>
</tr>
<tr>
<td>3.3.1 Argument and Research Questions</td>
<td>63</td>
</tr>
<tr>
<td>3.3.2 Research Design for the VFT Phase of the Study</td>
<td>64</td>
</tr>
<tr>
<td>3.3.2.1 Data Analysis for the VFT Phase</td>
<td>66</td>
</tr>
<tr>
<td>3.3.2.2 Evaluation of the VFT Phase</td>
<td>68</td>
</tr>
<tr>
<td>3.3.3 Research Design for the Design Science Phase</td>
<td>69</td>
</tr>
<tr>
<td>3.3.3.1 Problem Identification and Motivation</td>
<td>70</td>
</tr>
<tr>
<td>3.3.3.2 Define Objectives for a Solution</td>
<td>71</td>
</tr>
<tr>
<td>3.3.3.3 Design and Development of Artifact</td>
<td>71</td>
</tr>
<tr>
<td>3.3.3.4 Demonstration of Design Artifact</td>
<td>75</td>
</tr>
<tr>
<td>3.3.3.5 Evaluation of Design Artifact</td>
<td>75</td>
</tr>
<tr>
<td>3.3.3.6 Communication of the Design Science Study</td>
<td>78</td>
</tr>
<tr>
<td>3.4 Conclusion</td>
<td>79</td>
</tr>
</tbody>
</table>
4 Privacy Objectives for Cloud Computing

4.1 Introduction 81
4.2 Making Values Explicit 81
4.3 Data Analysis 82
4.4 Results 84

4.4.1 Fundamental Objectives for Cloud Privacy 87
4.4.1.1 Increase Trust with Cloud Provider 87
4.4.1.2 Maximize Identity Management Controls 90
4.4.1.3 Maximize Responsibility of Information Stewardship 92
4.4.1.4 Maximize Individual’s Understanding of Cloud Service Functionality 94
4.4.1.5 Maximize Protection of Right to Privacy 97
4.4.1.6 Maintain Integrity of Data 100

4.4.2 Means Objectives for Ensuring Cloud Privacy 101
4.4.2.1 Maximize effectiveness of Secure Data Transfers 101
4.4.2.2 Optimize Ease of Use of Cloud Technology 102
4.4.2.3 Maximize Technology Infrastructure Competencies 103
4.4.2.4 Minimize Unnecessary Access to Information 104
4.4.2.5 Increase Standardization of Cloud Technologies 105
4.4.2.6 Optimize Effectiveness of Privacy Policy Governance 107
4.4.2.7 Maximize Performance of Privacy Risk Assessments 108
4.4.2.8 Increase Control Over Information Disclosure 110
4.4.2.9 Ensure CSP has Effective HR Practices 111
4.4.2.10 Minimize Government Access to Information 112
4.4.2.11 Maximize Effectiveness of Independent Oversight of Privacy Practices 114
4.4.2.12 Optimize Access Controls 115
4.4.2.13 Optimize Segregation of Information 117
4.4.2.14 Minimize Third Party Access to Information 118
4.4.2.15 Minimize Liability Concerns 118
4.4.2.16 Ensure Cloud Service Provider has Effective Internal Controls
4.4.2.17 Maximize Availability of Cloud Resources
4.4.2.18 Increase Awareness of Data Ownership
4.4.2.19 Ensure Service Level Agreements Meet Privacy Requirements
4.5 Evaluation of cloud privacy objectives
4.6 Discussion on the cloud privacy objectives
4.7 Conclusion

5 Designing a Cloud Privacy Audit Framework

5.1 Introduction
5.2 Problem Identification: Analyzing Privacy in the Cloud
5.3 Objectives of a solution: Creation of Cloud Privacy Audit Framework
5.4 Development and design of the artifact: Constructing a Cloud Privacy Audit Framework
5.5 Demonstration of the Cloud Privacy Audit Framework
5.6 Evaluation: Findings and limitations of the Cloud Privacy Audit Framework
5.6.1 Perceived Usefulness and Perceived Ease-of-use of Artifact
5.6.1.1 Perceived Usefulness
5.6.1.2 Perceived Ease-of-use
5.7 Communication of the Contribution of the Design Science Study
5.8 Summary
## 6 Discussion

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1 Introduction</td>
<td>156</td>
</tr>
<tr>
<td>6.2 Cloud Privacy Strategy</td>
<td>157</td>
</tr>
<tr>
<td>6.2.1 Strategic Planning for Cloud Privacy</td>
<td>158</td>
</tr>
<tr>
<td>6.2.2 A synthesized perspective on the development of a cloud privacy strategy</td>
<td>160</td>
</tr>
<tr>
<td>6.2.2.1 Comprehensiveness</td>
<td>161</td>
</tr>
<tr>
<td>6.2.2.2 Formalization</td>
<td>163</td>
</tr>
<tr>
<td>6.2.2.3 Focus</td>
<td>164</td>
</tr>
<tr>
<td>6.2.2.4 Flow</td>
<td>165</td>
</tr>
<tr>
<td>6.2.2.5 Participation</td>
<td>167</td>
</tr>
<tr>
<td>6.2.2.6 Consistency</td>
<td>168</td>
</tr>
<tr>
<td>6.2.3 Summary</td>
<td>168</td>
</tr>
<tr>
<td>6.3 Evaluation of Cloud Privacy Practices</td>
<td>169</td>
</tr>
<tr>
<td>6.3.1 Synthesized Perspective of the Evaluation Process</td>
<td>170</td>
</tr>
<tr>
<td>6.4 Auditing Cloud Privacy Practices</td>
<td>172</td>
</tr>
<tr>
<td>6.5 Conclusion</td>
<td>175</td>
</tr>
</tbody>
</table>

## 7 Summary

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.1 Introduction</td>
<td>177</td>
</tr>
<tr>
<td>7.2 Summary of Research Performed</td>
<td>178</td>
</tr>
<tr>
<td>7.2.1 Value Focus Thinking Phase of Study</td>
<td>178</td>
</tr>
<tr>
<td>7.2.2 Design Science Phase of Study</td>
<td>179</td>
</tr>
<tr>
<td>7.3 Contributions of this Thesis</td>
<td>180</td>
</tr>
<tr>
<td>7.3.1 Theoretical Contributions</td>
<td>181</td>
</tr>
<tr>
<td>7.3.2 Methodology Contributions</td>
<td>182</td>
</tr>
<tr>
<td>7.3.3 Practical Contributions</td>
<td>183</td>
</tr>
<tr>
<td>7.4 Limitations</td>
<td>184</td>
</tr>
<tr>
<td>7.5 Future Research Directions</td>
<td>187</td>
</tr>
</tbody>
</table>
Appendix A: Interview Questions 189
Appendix B: List of Sub-Objectives for Cloud Privacy 190
References 194
Abstract

The rapid expansion of cloud technology provides enormous capacity, which allows for the collection, dissemination and re-identification of personal information. It is the cloud’s resource capabilities such as these that fuel the concern for privacy. The impetus of these concerns are not too far removed from those expressed by Mason in 1986, when he identified privacy as one of the biggest ethical issues facing the information age. There seems to be continuous ebb and flow relationship with respect to privacy concerns and the development of new information communication technologies such as cloud computing.

Privacy issues are a concern to all types of stakeholders in the cloud. Individuals using the cloud are exposed to privacy threats when they are persuaded to provide personal information unwantedly. An Organization using a cloud service is at risk of non-compliance to internal privacy policies or legislative privacy regulations. The cloud service provider has a privacy risk of legal liability and credibility concerns if sensitive information is exposed. The data subject is at risk of having personal information exposed. In essence everyone who is involved in cloud computing has some level of privacy risk that needs to be evaluated before, during and after they or an organization they interact with adopts a cloud technology solution. This resonates a need for organizations to develop privacy practices that are socially responsible towards the protection of their stakeholders’ information privacy.

This research is about understanding the relationship between
individual values and their privacy objectives. There is a lack of clarity in organizations as to what individuals consider privacy to be. Therefore, it is essential to understand an individual’s privacy values. Individuals seem to have divergent perspectives on the nature and scope of how their personal information is to be kept private in different modes of technologies. This study is concerned with identifying individual privacy objectives for cloud computing. We argue that privacy is an elusive concept due to the evolving relationship between technology and privacy. Understanding and identifying individuals’ privacy objectives are an influential step in the process of protecting the privacy in cloud computing environments.

The aim of this study is to identify individual privacy values and develop cloud privacy objectives, which can be used to design a privacy audit for cloud computing environments. We used Keeney’s (1992) value focused thinking approach to identify individual privacy values with respect to emerging cloud technologies, and to develop an understanding of how cloud privacy objectives are shaped by the individual’s privacy values. We discuss each objective and how they relate to privacy concerns in cloud computing. We also use the cloud privacy objectives in a design science study to design a cloud privacy audit framework. We then discuss the how this research helps privacy managers develop a cloud privacy strategy, evaluate cloud privacy practices and develop a cloud privacy audit to ensure privacy. Lastly, future research directions are proposed.
Chapter 1 Introduction

1.1 Introduction

This research is about understanding privacy objectives for ensuring cloud privacy. There is a lack of clarity in organizations as to what are individuals’ privacy expectations when using cloud technologies. This ambiguity with respect to individual’s privacy expectations in the cloud has also resulted in an uncertainty of privacy objectives for organizations operating in the cloud. In order for management to operate effectively, there needs to be a clear understanding of all potential issues. This includes cloud privacy issues from both the cloud service provider and user perspectives; otherwise the potential benefits from cloud technology will not be realized.

Cloud computing is positioned to be the next big information technology advancement. Why is cloud computing positioned for such growth and acceptance in the market place now? It is because with the evolution of information technology the value of information has increased. This has resulted in organizations demanding the utilization of more data than ever before. This demand for information has resulted in a 54% growth, in data storage (Chen and Yoon, 2010). In addition, the advancement in IT capabilities has resulted in a higher demand for powerful and faster processing capacity (Chen and Yoon, 2010). Organizations are finding it difficult to meet new technology demand due to limited resources. With advancement in technologies and the lower cost of connectivity, cloud computing is becoming a viable solution to meet these business needs.

However, there is a growing concern for the collection, dissemination and re-identification of personal information capabilities taking place in the cloud, and it is no
wonder that the cloud is facing challenges of ensuring information privacy (Dinev et al., 2009; Chen and Yoon, 2010). Privacy is a significant concern in the emerging context of cloud computing (Dhillon and Kolkowska, 2011; Chen and Yoon, 2010). The public concern for cloud technologies is a good example of how privacy issues arise from the development of new technologies. Rapid technological advancements that easily allow privacy infringements are widely in use today. One example of this is technology developed by Google, which creates a back door to Safari privacy controls so they could track the web activity of individuals who clicked on their ads. Advancements such as this supports the idea that cloud service providers need to be monitored to protect the privacy rights of their customers. Companies face reputation risks, which could lead to costly litigation and the defection of customers to the competition if they are exposed as a privacy misfit (Cavoukian and Hamilton, 2002). Privacy considerations need to be at the forefront of management’s concerns for all organizations considering adopting cloud technologies.

Organizations operating in a cloud environment need to ensure public trust by aligning or developing privacy policies with individuals’ privacy values and objectives (Mai, Menon and Sarkar, 2010; Hann et al., 2007). Having an independent audit performed is one way to establish and build trusting relationships between organizations and their stakeholders. An independent audit helps to ensure that the organization is adhering to their stated policies and regulatory requirements. However, currently there are no existing privacy standards or privacy audit frameworks for cloud computing. There is a need to develop a cloud privacy audit framework to ensure that individuals’ privacy objectives are met. It is beneficial to obtain an understanding of
personal information privacy objectives in the context of cloud computing. An understanding of privacy objectives will provide a good foundation for the development of a privacy audit framework for cloud computing. Our research develops an understanding of individual’s privacy values and personal information privacy objectives, as a means to identify cloud privacy objectives. These objectives are essential for the future development of a privacy audit framework for cloud computing.

The remainder of this chapter proceeds as follows. Section 1.2 presents the problem domain by introducing the importance of the relationship between technology and privacy. Section 1.3 presents the main concepts and definitions utilized in this research. Section 1.4 describes the research argument and presents the proposed research questions. Lastly, section 1.5 offers a description of the remaining chapters of the dissertation.

1.2 Problem Domain: The Relationship Between Technology and Privacy

Technology is often the catalyst of large-scale societal shifts in our culture. Marshall (1999, p 88) found “new technologies change our world view, our social interaction patterns, and our relationships to one another.” This is because the way individuals interact with each other changes as innovative technologies are introduced to the market. Consider the impact cell phone has had in the last couple of decades. Before cell phones were introduced, we did not have the expectation that we could immediately contact anyone we wanted. The cell phone changed this expectation. Now with smart phones we are developing the expectation that desired information should be at our fingertips 24/7. However, a cost of this information availability is resulting in a loss of privacy because information providers are collecting and selling information
about us as a means to generate a new revenue stream. Weiser’s (1991) claim that advancements in information technologies continue to be evermore pervasive within our society could not be any truer than it is today. Marshall (1999) posits that rapid advancements in technologies such as the Internet have not been matched by development of ethical guidelines for its utilization fast enough to maintain a proper balance between technology and individual rights. Prosser (1960) claimed that new technologies have given rise to a broad array of new privacy issues. This claim was re-enforced by Junglas, Johnson and Spitsmuller, (2008) and Westin (2003) who established that concern for information privacy co-evolves with technology advancements.

In recent years, emergent technologies such as Google and Facebook have strongly impacted our "privacy expectations" and how we interact with each other (Dinev, Xu and Smith, 2009). These social computing platforms are examples of how emerging technology can disrupt traditional norms of how users interact online and how information is generated, shared and distributed (Dinev et al., 2009). In essence, the contextual aspects of how users are interacting with each other is changing and so is their view of privacy because they are experiencing new threats. We believe that it is essential to this study to recognize the dynamic nature of the interaction between these items. Research has shown that individuals are constantly weighing their desire for privacy against their desire to interact with others by sharing personal information through various forms of communication (Kimmel, 1996; Sheehan 2002). This weighing process involves making minor adjustments to their privacy values based on various contextual situations (Kimmel, 1996). Even the notion of privacy itself has been found to change depending on the nature of its threats (Regan 1995; Sheehan 2002). Research
as found that context has either a moderating influence (Bellman et al. 2004; Dinev et al. 2006; Smith et al. 1996) or a direct influence (Malhotra et al., 2004) on an individual’s view of privacy (Smith, Dinev and Xu, 2011). Privacy is a significant concern in the emerging context of cloud computing (Dhillon and Kolkowska, 2011; Chen and Yoon, 2010). We posit that the concept of privacy within cloud computing is evolving with respect to the threats to privacy in the cloud environments which adds to its uncertainty.

Privacy issues are a concern to all types of stakeholders in the cloud. An individual using the cloud is exposed to privacy threats when they are persuaded to provide personal information unwantedly. An Organization using a cloud service is at risk of non-compliance to internal privacy policies or legislative privacy regulations. The cloud service provider has a privacy risk of legal liability and credibility concerns if sensitive information is exposed. The data subject is at risk of having personal information exposed. In essence everyone who is involved in cloud computing has some level of privacy risk that needs to be evaluated before, during and after they or an organization they interact with adopts a cloud technology solution. We are concerned that the rapid expansion of cloud computing is occurring faster than the development of best practices that ensure ethical standards are maintained. This resonates a need for organizations to develop cloud privacy audit practices to verify that they are being socially responsible towards the protection of their stakeholders’ privacy.

1.3 Concepts and Definitions

The purpose of this section is to clarify several definitions, which are integral to this dissertation. The concept of privacy has been heavily debated and will be covered in
greater detail in the literature review chapter; however, a brief introduction of the privacy concept is pertinent to continuation of this discussion. Privacy has been identified as one of the most important ethical issues of the information age (Mason 1986). Privacy has become an influential topic for managers who are concerned about maintaining their customer base (Culnan and Armstrong, 1999; Smith, 1993). Smith (1993) expressed information privacy to be concerned with the information data collection process, information errors, secondary use of information and unauthorized access to information. Personal information privacy has been defined as the ability of the individual to control information about oneself (Stone et al., 1983; Milburg, Burke, and Smith, 1995). Individuals desire the right to ensure that personal information is not collected, used or disseminated to unauthorized third parties. For the purpose of this study, we define personal information privacy as the ability individuals have to control transactions that regulate access to information about one’s self, such that it reduces vulnerability and unwanted disclosure of personal information.

The concept of values has been researched from many different perspectives, which we will cover in greater detail in chapter two as part of the literature review discussion on value research. However it is essential to note certain aspects of value research here, which informed our definition of values and individual values as they relate to this thesis. One such aspect of value research of concern originated in 1928 with the German psychologist Eduard Spranger. This stream of research focused on the classification of human beings based solely on the things they value.

Spranger’s classification of types of man sparked an interest among researchers, and they began to focus on the individual’s values and end state preferences.
Rokeach (1973: p. 160) stipulated “once a value is internalized it becomes, consciously or unconsciously, a standard or criterion for guiding action, for developing and maintaining attitudes toward relevant objects and situations, for justifying one’s own and other’s action and attitudes, for morally judging self and others, and for comparing self to others.” Therefore, values are utilized to form a decision in a given context. Values that are of concern to the decision maker are made explicit by the identification of objectives. Keeney (1992) defined an objective as a statement of something one desires. Three features characterize an objective: a decision context, an object, and a direction of preference. For the purpose of this thesis, we define individual privacy values as an individual’s own unique set of values that allow them to achieve desirable end states such as a desired privacy objective.

Cloud computing is an evolving concept especially with the recent advancement of emerging technologies. Several researchers have tried to define cloud computing; however, there is no agreed upon definition. We will cover these various definitions in greater detail in the literature review section. For the purpose of this study, we utilized the following National Institute of Standards and Technology (NIST) definition for cloud computing. “Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction” (Mell and Grance, 2009). Cloud-based applications are quickly becoming standard starting applications for emerging technology companies (Chen and Yoon, 2010). The main benefit from the cloud is that it provides an opportunity, quickly and easily, to collaborate and access data from anywhere with Internet access while saving
money on capital expenditures by paying for only resources that are being used.

1.4 Research Argument and Proposed Research Questions

In order to ensure the protection of personal information in the cloud, we argue that it is important to understand individuals’ privacy values and their cloud privacy objectives. Understanding and identifying individuals’ privacy values with respect to cloud privacy objectives is important for the development of an organization’s cloud technology strategy. Organizations need to recognize their customer’s cloud privacy expectations in order to develop socially responsible privacy practices. A benefit from this understanding is that organizations utilizing cloud technologies could create privacy policies that meet customers’ expectations of cloud privacy objectives.

Privacy in the cloud is an elusive concept due to the evolving nature of the relationship between technology and privacy discussed above. This evolving relationship between privacy and technology is only part of the problem for comprehending the true meaning of privacy. The concept of privacy is in a constant state of flux (Solove, 2006), which attributes to its ambiguity (Culnan and Williams, 2009). Another challenge to understanding what encompasses privacy is that privacy is context specific and dynamic in the sense that it varies with life experiences (Xu et al. 2008; Altman 1977; Laufer and Wolfe 1977). This suggests that privacy values are unique for each individual.

There is a lack of clarity in what organizations need to do in order to protect individuals’ privacy (Mason, 1986; Culnan and Williams, 2009). This is a result of not having well defined objectives for ensuring personal privacy. Culnan and Williams (2009) suggest the need for information privacy researchers to study; how organizations should handle personal identifiable information, what are organizations
responsibilities towards information privacy protection, the moral duties organizations have to protect their customers and stakeholders privacy needs. Conducting research along these lines would help organizations and researchers develop comprehensive privacy policies to ensure information privacy.

This study uses Keeney’s (1992) value focused thinking (VFT) approach to identify individual privacy values with respect to emerging cloud technologies, and to develop an understanding of how cloud privacy objectives are shaped by individuals’ privacy values. Keeney (1988b) claims that values are important for many aspects the decision-making process including, guiding information collection process, evaluating alternatives, creating alternatives and identifying and resolving conflicts. One goal of this study is to develop an understanding of the relationship between individual privacy values and cloud privacy objectives. Another goal is to develop a privacy framework for ensuring cloud privacy.

The focus of the research leads to the following research questions:

1) What are privacy objectives for cloud computing?
2) How can an audit for cloud privacy be designed?

1.5 Dissertation Structure

In this first chapter, the nature of the research problem was outlined, and the research questions were established. Chapter two is a literature review of values and privacy research. The aim of this review is to evaluate the current body of literature with respect to privacy values and to consider its implications for the emerging cloud environment. Chapter three discusses the theoretical basis for addressing the research questions. In addition, we present the research methodology and research
design of the study. In chapter four, we present the results of the first phase of this study in the form of means and fundamental objectives and discuss their implications within the context of cloud computing. Chapter five will present a framework for auditing information privacy within cloud computing environments. Chapter six will discuss the findings of this study in position it within the existing privacy literature. In chapter seven, we will discuss the contributions of this study to both the research community and its usefulness to practitioner application.

The creation and adoption of new technology is often a catalyst for large-scale societal change. This statement could not resonate more true than with advancements in cloud computing technologies. As new innovative technologies are introduced into our society the methods in which people interact or communicate with each other very often are affected. A prime example of this is with the recent introduction of cloud technologies. With the adoption of cloud computing, organizations are entrusting data to be managed by external parties on remote servers “in the cloud.” The single greatest fear of cloud clients according to Takabi et al. (2010) is the storage of their data and applications on systems that reside outside of their control. However organizations are still increasingly migrating their systems to the cloud because of the promised scaled economic benefits associated with being able to provision computing resources on demand (Chen and Yoon, 2010). This migration of workspace to shared infrastructure environments increases the risk of exposure to private and personal information and raises privacy and confidentiality concerns (Ryan, 2011; Takabi, Joshi and Ahn, 2010). Privacy is a core issue in cloud computing environments and is a good example of how privacy issues arise from the development of new technologies.
The problem domain for this study is framed by the recent advancements of cloud technologies and the lack of privacy standards or best practices to ensure ethical standards with respect to privacy are maintained.
Chapter 2 Literature Review

2.1 Introduction

This chapter reviews literature relevant to our argument. We argue individual values are important in defining objectives for ensuring privacy in cloud computing. In support of this argument there are two informing literatures that are relevant to this study. One is the research literature on values and the other is the research literature on privacy. In order to systematize these bodies of literature it is helpful to utilize frameworks, or heuristics, for understanding them, which best fit with the nature of this study’s analysis. Only after such a synthesis can we assess the status and directions of the current literature on our research topic. Mitnick (1994; p. 114) stated that to create order out of confusion, “We select and order abstractions [of the world] that are said to grant us “understanding”. It is an error to claim that only theory does this; antecedent to every theory is an ordering of abstractions that constitutes a choice of how to depict which elements of the real world and how such elements are related to one another. These distincional choices are critical in the promoting the basic understanding that is sought.”

Following Mitnick’s advice, we adopt the following frameworks to systematically approach the vast extent of literature on values and privacy. A level of analysis framework was used to classified value research literature based on where the values in the study were held or exercised (i.e. individual, organizational or societal values). Rousseau (1985) espoused this approach as the one with the greatest potential for examining the vast amount of literature on values. The second framework is a means of classification designed to assist us in the learning process about privacy. We classified privacy articles into the following sub-topics: privacy and ethics, society and privacy,
location based privacy, data/database privacy, online privacy, and cloud privacy.

The remainder of this chapter is divided into three sections. Following the introduction, the first section discusses the literature on values research. The second section discusses the research literature on privacy. The third section presents the gaps in the literature as identified in the review and positions this study within the extent literature.

2.2 Values Literature Review

The concept of values is an important construct in social science research (Agle and Caldwell, 1999). A review of the literature shows that most of the early social scientists work on the concept of values held to a more rigid view derived from its Latin roots where “valere” means to be worth (Spates, 1983). Most of these early works were building upon the likes of Adam Smith (1776), and Karl Marx (1848) and their view towards the value of labor in the market economy. This pure economic view towards the concept of values started to evolve beyond this simplistic view with the emergence of the sociology discipline. The works of sociologists like Small and Vincent (1894), Giddings (1907) and Sumner’s (1906) played a significant role in influencing our view towards the role of values in our society by introducing concepts such as a “common will” and “social mind”.

Ravlin and Meglino (1987) found that values exert influence on human cognition, behavior and attitudes. Values are important for establishing, monitoring, and maintaining relationships between individuals, organizations and societies (Agle and Caldwell, 1999). For the remainder of this review of value literature we will focus on the literature along these three levels: individual, organizational and societal
2.2.1 Individual Level Perspective of Values

The foundation for most contemporary research with a focus on individual values draws its influence from the work of Eduard Spranger’s 1928 titled “Types of Men”. Spranger identified six types of men based on what attributes they valued the highest. Spranger’s classification of types of men sparked an interest among researchers as they began to focus on understanding the concept and implications of individual’s values. Rokeach (1973) describes values as “determinates of virtually all kinds of behavior that could be called social behavior or social action, attitudes and ideology, evaluations, and moral judgments and justifications of self and others, comparisons of self with others, presentations of self to others, and attempts to influence others” (p. 5). He claimed that individual values are concerned with preferred end states such as social recognition, an exciting life, a world at peace and equality.

Keeney (1988a) considered values to be important in every aspect of human behavior. Values are what we as individuals care about and they should be at the core of our decision process (Keeney, 1992). Kluckhohn (1951: p. 396) expressed that “values become instigators of behavior ‘within’ the individual.” In essence, values are internalized by individuals and guide their behaviors. Parsons (1951) also considered the importance of values in determining the actions or behaviors of individuals in his development of a general theory of action.

Research shows that values have a substantial influence on the behavioral responses of individuals (Rokeach, 1973; Meglino and Ravlin, 1998). Researchers have adopted several theoretical viewpoints as a means to investigate the influence of
individual values on behavioral choices. One such theory is Behavior Decision Theory (BDT), which has been used by many disciplines to study the relationship between values and decision-making processes (Einhorn and Hogarth, 1981). BDT is grounded in the assumption that human behavior is governed in large measure by value. One fundamental assumption of BDT is that if the decisions that men take as decision makers are the decisions they should take, then men can be said to be acting rationally. Because actual choice can differ from prescribed choice, a distinction is sometimes made between normative and descriptive decision theory. The rational decision-making process is theoretically addressed in the literature by normative decision theory, whereas the choices actually made in a given situation falls in the realm of descriptive decision theory (Barron 1974). BDT is primarily concerned with this dichotomy between normative and descriptive aspects of decision-making (Slovic et al., 1977). In essence behavior decision theorist believe that there is a linear approach to deducting the best choice among a selection of alternative options based on an individual’s value of the alternatives.

A second theory commonly used to understand the relation between values and individual behaviors is Means-Ends Chain (MEC) theory. MEC theory is a model, which represents the linkages between attributes, consequences, and values. Gutman (1979) claims that knowledge is maintained in an individual’s memory bank, which is representative of a hierarchical cognitive structure with various levels of abstraction. A model of an individual’s cognitive structure would represent all of the different levels of abstraction an individual maintains with regards to personal knowledge. Rokeach (1968) suggested that such a model would offer a theoretical and conceptual foundation for
connecting individual’s values to their behavior.

A Means–Ends Chain is defined as consisting of an interconnected set of cognitive elements that allows a person to select objects or activities that enable an individual to achieve their desired end states. Gutman (1982) suggests that two major events need to occur before the development of a means-end chain can occur. The first event, crystallization of values, allows individuals to internalize their own values to the point where they are articulated into goals or valued states. The second event that needs to occur is a clustering of lower level object attributes or values at the bottom of the chain to limit the complexity of the choice situation to acceptable levels. Thus, the means-end chain permits us to focus on the basic values individuals have in life while not losing sight of how these values influence choices in specific situations. These objects or values have to be given meaning in terms of the internal coding system established by the individual for making sense of the world (Olson and Muderrisoglu, 1979).

Senger (1971) suggested that “personal value structures and systems of preference ordering used by decision-makers could lead to more useful decision models, which are better able to predict choice behavior.” (p.422) Similarly Keeney (1988a) stated that building a value model to structure and analyze the problem domain is important in the decision-making processes. A model of an individual’s cognitive structure would represent all of the different levels of abstraction an individual maintains with regards to personal knowledge. Rokeach (1968) suggested that such a model would offer a theoretical and conceptual foundation for connecting individual’s values to their behavior. It is also important to note that individual values are unique in the sense that
they vary with each individual because their life experiences are unique to them.

It is also important to note that the context in which a decision is made is equally important as the value in determining the outcome. In his proposal for a Theory of Value, Catton (1959) suggested a concept of value-space as a means to analyze the relationship between individual’s values and their behavior. Catton (1959) claimed that “when values are held constant, the order of preferences among a set of desiderata may nevertheless vary from person to person or from group to group as a result of the failure of each person or group to be fully cognizant at all times of all the dimensions of value-space” (p. 317). These varying results in the ordering of preferences among desiderata can be helpful to explain the uncertainty that exist in privacy expectations of individuals which is the subject matter of this study.

2.2.2 Organizational Level Perspective of Values

The organizational perspective of values has been a subject area of study for decades. Within the scope of the business literature, research topics such as managers decision-making process (England, 1967, Meglino and Ravlin, 1998), management success (Jaskolka, Beyer, & Trice, 1985); individual - organization fit (Chatman, 1989); organizational commitment (Wittig-Berman & Lang, 1990), moral reasoning (Weber, 1993), ethical decision making (Akaah & Lund, 1994); and customer behavior (Keeney, 1999) have been investigated.

These research studies show that values are important to corporate success and that there is a positive relationship between shared values and organizational performance (Gordon and DiTomaso, 1992; Denison, 1990). In his study of value
structures, Parsons (1956; p. 63) defined an organization “as a social system oriented to the attainment of a relatively specific type of goal, which contributes to a major function of a more comprehensive system, usually the society.” He further expounded, “such an organization is analyzed in terms of an institutionalized value system, above all defining and legitimizing its goal, and the mechanisms by which it is articulated with the rest of the society in which it appears” (Parsons, 1956; p. 63). In this section of the review we identified several research streams within the organizational values research literature, which are relevant to this study. We classified these themes as follows: decision-making, corporate culture, business ethics. In the remainder of this section we will discuss various value concepts found within these streams of research in greater detail.

Organizational decision-making process is a popular research domain within the field of organizational value research. Everyday, as individuals, we make choices that affect our lives and those around us and the same is true for organizations. In their observations of executive management teams Guth and Tagiuri (1965; p. 123) claimed that “personal values are important determinates in the choice of corporate strategy.” McGuire et al. (2006) noted the notion of a socially constructed reality and the contextual nature of decision-making and the important role played by values in driving decision-making processes. Including values earlier in the decision-making process will result in a better selection of alternatives for decision problems (Keeney, 1992). In his quest for a sociological approach to the Theory of Organizations, Parsons (1956) was concerned with understanding the core processes of making decisions within organizations. By understanding an organization’s decision-making process we can hopefully improve
future decision outcomes for the organization by knowing how to analyze the decision problem.

Keeney (1992) extended the use of values in the decision making process with his development of value focused thinking approach to developing alternatives in the decision making process. Keeney (1992; p. 33) states that “values are what we care about and they should be the driving force for our decision making.” Focusing on values in the decision-making process increases the number of decision options within the problem context because it is not restricted to only known options.

Corporate culture has also been a popular research topic in the management literature since the early 1980s (Hofstede, 1998). There are many definitions of organizational culture and most of these mention culture and values as being integral to each other. The concept of corporate culture has evolved from the literature on organizational climate. Litwin and Stringer (1968: p. 1) defined ‘organizational climate’ as “a set of measurable properties of the work environment, perceived directly or indirectly by the people who live and work in this environment and assumed to influence their motivation and behavior.” Corporate culture has been described as having a characteristic of the organization that is manifested in and measured from the verbal and/or nonverbal behavior of individuals and aggregated to the level of their organizational unit (Hofstede, 1998). Schein (1985) described organizational culture as the existence of shared meanings, beliefs, and values with values being at the core. Values are viewed as an important aspect of organizational culture (O’Reilly and Chatman, 1996).

Tichy (1982) defined organizational culture as shared values. A strong set of corporate values help employees identify with the organization’s goals and
provide an opportunity to align organization’s leadership and its employees (Ghosh, 2008). Hofstede (1998) proclaimed that while no simple one-to-one relationship between any aspect of corporate culture and organizational performance it is obvious that organizational culture affects performance. Corporate culture is considered to be a decisive influence on the survival or failure of an organization (Hofstede, 1998).

Another important stream in the organizational value research domain is concerned with business ethics and corporate responsibilities. Theoretical constructs examined within this domain include topics such as organizational ethical climate (Victor and Cullen, 1988; Dickson, Smith, Grojean and Ehrhar, 2001), ethical codes of conduct (Somers, 2001), corporate social responsibility (Aupperle, Carroll and Hatfield, 1985; Carroll, 1999; Joyner and Payne, 2002). Research has shown that ethical philosophies and values of management have a strong influence on the ethical choices and behaviors of employees (VanSandt and Neck, 2003; Ghosh, 2008).

In their studies of ethical climates, Victor and Cullen (1988) identified the following three ethical climates: egoistic, benevolent and principled. An egoistic climate exists when the norms of a company supports the satisfaction of self-interest and ignores the needs or interests of others. A benevolent climate exists when the norms of a company supports maximizing the interest of others. A principled climate exists when decision makers develop decisions that are based on adherence to rules and codes when faced with ethical dilemmas. These climates can be derived internally by individuals based on their moral compass or by external drives such as an ethical code or integrity of an organization or on a higher level such as a law or religion.
Research interest in understanding what influences ethical decisions led Zalkind (1987) to examine the role of corporate culture and stated organizational values in the context of understanding how corporate codes of ethics influence the ethical dimension of employee behavior. With the decline of corporate ethics there is an increased interest in the relationship between the perception of wrongdoing in the organization and the presence or absence of corporate codes of ethics (Somers, 2001). Corporate codes have been found to inhibit unethical behavior in organizations (Tsalikis and Fritzche, 1989; Murphy et al., 1992). Weeks and Nantel (1992) suggests that organizations that have adopted codes of ethics empower ethical decision-making among their employees thereby leading to positive work attitudes and possibly to higher levels of organizational commitment. Organizations concerned with ethical conduct should establish a supportive environment where corporate values emphasize integrity and ethical conduct and that engenders commitment to those values.

2.2.3 Societal Level Perspectives of Values

With the recent move towards globalization studies along the society level with respect to values has been on the rise. Keeney (1988b) espoused a need to obtain and synthesize public values as a means for developing better public policies. Hofstede and Bond (1984) utilized a modified version of the Rokeach Value Survey and found five dimensions for work-related values among employees in international companies that have helped to establish the importance of understanding the influence of societal values on the health of an organization.

The research on values at the societal level has focused primarily the interaction between societal values and organizational behavior (Dowling and Pfeffer,
1975; Hofstede and Bond, 1984). Dowling and Pfeffer (1975; p. 122) claim
“organizations seek to establish congruence between the social values associated with or
implied by their activities and the norms of acceptable behavior in the larger social
system of which they are a part.” This view is aligned with Bowen’s (1953) claim that
social responsibility is dependent on the values and objectives of society. Bowen’s
concept of social responsibility relies on corporations or government agencies
maintaining the concept of moral agency and behaving according to society’s values
(Wartick and Cochran, 1985). There is a growing requirement for managers to
assume responsibility for the public good, as he determines his actions based on
ethical standards of conduct (Drucker, 2002). There is research that supports the
argument that organizations will fail if their prevailing culture and values are congruent
with those of society (Sims, 1992).

The main focus of the research in the societal level of values research is
concerned with ethical and corporate responsibilities. Within the corporate social
responsibility (CSR) literature Joyner and Payne (2002) argued that if ethical and
socially responsible behavior can be shown to boost financial results then many
organizations might implement real changes towards becoming more socially
responsible. Research has shown that the concepts of values, ethics, and corporate
social responsibility are not independent of each other they are in fact intertwined
with each other (Carroll, 1979; Joyner and Payne, 2002). The extent to which a
corporation’s perceived social responsibility is influenced by their organizational
values, which are based on the accepted norms of society, helps explain this
dependency. Corporate social responsibility has been defined as the responsibility of a business entity to adapt to the values and expectations of society (Andrews, 1987; Carroll, 1979, Sethi, 1975).

Carroll (1979) developed the Organizational Social Performance Model framework, which integrates the levels of responsibility, social issues and the firm’s social responsiveness to these issues, as means to assist organizations in making ethical decisions aligned with their corporate culture and the image they want to project. Jackson (2000) noted that the transparency and perception of corporate values toward ethical issues within an organization ultimately influences managers’ attitudes towards making ethical decisions.

There is a growing recognition that good ethics can have a positive economic impact on the performance of firms (Joyner and Payne, 2002). Drucker (1954) stated that public responsibility is a key area in which business objectives should be set. He also posited that an organization’s first responsibility to society involved making a profit however organizations need to consider the impact of every business policy and action upon society (Drucker 1954). This sentiment is also resonated by Porter and Kramer (2006) fifty years later when they stated “If corporations were to analyze their prospects for social responsibility using the same framework that guides their core business choices, they would discover that CSR can be much more than a cost, a constraint or a charitable deed – it can be a source of opportunity, innovation, and competitive advantage.” This research stream on corporate social responsibility is concerned with how to achieve a higher level of
“greater good” practices from organizations.

2.2.4 Theory of Values as a Theoretical Foundation

This study utilizes individual’s values to develop an audit framework for ensuring privacy in cloud computing environments. Therefore, understanding the concept of values and the impact they have on an individual’s behavioral decisions is an essential foundation to developing an informed discussion on our research questions. Keeney (1992) claims that values are important in every aspect of human behavior. He also provided evidence that the concept of a value construct has become important in all of the social sciences. Each discipline such as sociology, psychology, economics, management, and ethics has their own theoretical stance towards the concept of values. Initial works by sociologists like Small and Vincent (1894), Giddings (1907) and Sumner’s (1906) played a significant role in influencing our view towards the role of values in our society.

Parsons’ work in the development of Action Theory (1951, 1953) also helped to elevate the status of value analysis in sociology research (Spates, 1983). He built upon the works of Pareto, Durkheim and Weber claiming that all three were basically saying the same thing – that ideas founded in the morals of a culture are the determining and distinguishing elements of social existence. Parsons (1951) defined values as those moral beliefs to which people appealed for the ultimate rationales of action. Building on this notion of values being the rationale our actions, Kluckhorn (1951) developed the following definition “a value is a conception, explicit or implicit, distinctive of an individual or characteristic of a group, of the desirable which influences the selection from available modes, means, and ends of actions” (p. 395). Catton’s (1959)
theory of values is in agreement with these concepts of values, however he extends them with the notion that the given context and timing of the situation also influence individuals’ value preferences.

Catton (1959) proposes in his theory of values that, “the intensity of a person’s desire for a given object varies systematically from time to time, and that this intensity at any particular time is a function of the continuously perceived similarity of the object to other objects strongly desired at that time” (p. 315). Catton (1954) suggests that internalized values of individuals influence their behavior preferences. This is because an individual’s values help determine how much they desire something. A person’s desire for something, otherwise known as desideratum, is dependent on the individual perception of the situational context at hand (Catton, 1954; Rokeach, 1973). Basically each individual’s desideratum will change given the context. This implies that their choice of behavior may change depending on the given situation. Catton (1959) claims that individual’s choices of behavior maintain a regular pattern though time and are the result of some internal code which provide criteria for the individual to order the preference of various desiderata. This process of ordering preferences of desiderata Catton (1959) defines as behavior valuing. This process of ranking of values will result in a different value priority for each person therefore it is a challenge to meet everybody’s needs at the same time. It is important for decision makers to understand how this variation in values can affect individual value preferences.

Keeney (1992) proposes the use of values in the decision making process with his development of value focus thinking approach to developing alternatives in the
decision making process. Keeney (1992) claims “values are principles for evaluating the desirability of any possible alternative or consequence” and that “values are what we care about and they should be the driving force for our decision making.” Focusing on values in the decision-making process increases the number of alternative options because the alternative identification process is not restricted to only known options. This is achieved by considering what is important to “me” instead of thinking what are my existing options. A value focused thinking approach allows for the development of privacy objectives as a means to guide strategic decision on how to ensure individual’s privacy. A value focused thinking approach is concerned with understanding individuals values towards a decision problem within a given context or environment. This approach is aligned with an abductive research approach and therefore it is appropriate for this research study. Catton’s (1959) Theory of Value provides a strong theoretical foundation for the use of value focused thinking as a research method.

2.3 Privacy Literature Review

For this study we are interested in the relation between information technology and individual privacy objectives. Research has established that concerns for information privacy co-evolves with technology advancements (Junglas, Johnson and Spitsmuller, 2008; Westin, 2003). Furthermore, there appears to be an ever-widening gap between new technology and accepted ethical guidelines for their use such as the gap that exist between cloud technology and its ethical practices towards privacy.

In the spirit of Mitnick’s desire for classification to assist the learning process, we classified the literature into the following sub-topics: privacy ethics and society,
information privacy, location based privacy, online privacy, and cloud privacy. For the remainder of this section we provide a broad overview of the privacy debate then we will discuss the privacy research within the sub-topics as it relates to information technology.

2.3.1 Privacy Debate

The privacy debate started when Warren and Brandesis (1890) introduced the notion of a right to privacy in an article in the Harvard Law Review. They argued that the intensity and complexity of life within our advancing civilization has resulted in individuals retreating from interaction with their fellow man and society. Additionally they posit that the role of solitude and privacy is becoming more essential to the individual (Warren and Brandesis, 1890). The purpose of their legal debate was to consider whether the law supports a principle, which can be invoked to protect the privacy of the individual. Their argument established the right to privacy within the confines of tort law. Prosser (1960) and Post (1989) continued the legal debate on the rights of privacy. Prosser was able to successfully argue the importance of privacy and improve its legitimacy claims as a right within realm of common tort law (Richards and Solove, 2010). Post (1989) argued that the common law tort of invasion of privacy safeguards social norms. He posits, “the values of privacy, and the identity of persons and communities predicated upon those values, are thus endangered by the vast contemporary expansion of the public created by the mass media”. While the legal debate over an individual’s right to privacy is beyond the scope this study it is important to note, as it has been a strong influence in the concept of privacy.
Privacy as a concept is very complex and has been questioned in many other disciplines besides law such as sociology, psychology, management, and information systems. Researchers have considered multiple perspectives in their attempts to define privacy. These perspectives have ranged from a process view, psychological view, to a behavioral view (Margulis, 2003). Altman (1977) maintained a process perspective towards privacy in that he believed individuals regulated social interactions thereby selectively controlling access to one’s self.

A psychological perspective emphasizes privacy as a control over or regulation of scrutiny, surveillance or unwanted access (Allen, 1988; Margulis, 1977). Westin (1967) focused on information disclosure and defined privacy as an individual’s claim to be able to self-select when, how and to what extent their information is communicated to others. Westin (1967) considered privacy to an important aspect of an individual’s psychological development because it provides opportunities for self-assessment, individual development and personal autonomy with respect to their self-identity.

Margulis (2003) developed a behavioral perspective of privacy based on Altman’s (1977) and Westin’s (1967) definitions of privacy. In his analysis of their privacy theories he was able to identify two important factors of privacy: control over disclosure of personal information and a notion of vulnerability (Margulis 2003). According to Margulis (2003) privacy involves control over transactions that regulate access to self, such that it reduces vulnerability and increases decisional and behavioral options. The debate over the concept of privacy will continue to vary because its definition will depend on the context and viewpoint from which it is to be examined. For the purpose of this study we adopt Margulis’ behavioral view and define
personal information privacy, as the ability individuals have to control transactions that regulate access to one’s personal information, such that it reduces vulnerability and unwanted disclosure.

2.3.2 Privacy Ethics and Society

In exploring the ethical implications of the information age Mason (1986) identified privacy as one of the four primary ethical issues of the information age. Mason (1986) was concerned with “what information about one’s self or one’s associations must a person reveal to others?” (p. 5). He argued that two aspects of the information age pose a threat to our privacy; the first is the growth of information technology and its capabilities to capture and process information, second is the increased value of information in the decision making process. With the increased amount of information being collected by organizations Culnan and Williams (2009) argue that organizations have a moral obligation that extends beyond legal compliance to take reasonable precautions with consumer data and to avoid causing personal harm by misuse of their personal information. Research shows that organization’s privacy behaviors tend to be reactive and driven by external pressures such as regulatory factors instead of being proactive with their privacy practices (Goodhue and Straub 1991; Greenaway and Chan, 2005; Smith 1993). Culnan and Williams (2009) suggest that organizations develop principles based on shared moral values by which to guide the creation of privacy practices.

The concept of privacy is dependent on the current privacy values and norms that exist within society. Privacy as social issue has increased for Americans especially since 9/11 and the passage of the USA Patriot Act (Gandy, 2003). Margulis (2003)
examines privacy from three distinct positions: high-privacy position, balanced-privacy position and limited privacy position. The high-privacy position wants government to protect privacy rights. The balance-privacy position wants some government intervention along with voluntary organizational programs to encourage individual privacy. The limited-privacy position desires business efficiency and societal protection over individual privacy rights. The legal aspects of information privacy is very complex even though it is has been argued to be protected by the fourth amendment and several other state and federal privacy statutes such as the constitutional right to information privacy (Solove, 2006). Historically it has been the responsibility of individuals to create contracts with organizations such as healthcare providers for protection of their personal data (Smith, Milberg and Burke, 1996). Privacy contracts are a means to ensure that all parties involved have a clear understanding as to what their responsibility is towards the protection of the individuals’ or organization’s privacy.

2.3.3 Information Privacy

After Mason’s seminal work identifying privacy as one of the biggest ethical concerns for the information age, information systems researchers increased their focus on the notion of information privacy (Straub and Collins, 1990; Culnan, 1993; Milberg, et al., 1995). Studies have viewed privacy from many different perspectives such as a moral or legal right and the ability to control one’s personal information (Stone et al., 1983; Bélanger and Crossler, 2011; Clarke 1999). A main consideration with respect to information is with the control of information (Katzan, 2010). Straub and Collins (1990) considered the collection and dissemination of information on individuals while
respecting individual rights to privacy an important topic of concern. Organizations have typically argued that the organization that creates or maintains the information should have control of it. While, individuals believe that they should have the ability to control their identity and the release of information about themselves.

Within the information privacy literature, organizational practices, individual perceptions of these practices and societal responsibilities with respect to privacy have been linked in many ways (Smith et al, 1996). Clarke (1999) defines information privacy as “the interest people have in controlling, or at least significantly influencing, the handling of information about themselves”. The concept of information privacy has been difficult to quantify with a confirmatory empirical approach. Smith et al. (1996) developed an information privacy concern measurement scale as a proxy for information privacy. They identified the following four data-related dimensions of information privacy concerns: data collection, data errors, secondary use of data and unauthorized access to information. Due to the complexity and difficulty of defining privacy many researchers have opted to use the information privacy concern scale as a proxy for the concept of privacy (Dinev et al., 2009). While this acceptance has allowed for some advancement in the realm of privacy research there still is some concern that the information privacy concern scale is based on a negative notion of privacy and is thus not a true measure of privacy (Dinev et al. 2009).

2.3.4 Online Privacy

The ability of online websites or web application to track individual preferences,
behaviors, and identity is also a concern for individual’s privacy. With the pervasiveness of the Internet, the research topic of online privacy has been a very popular topic among researchers. Research topics such as information privacy concerns (Son and Kim 2008; Pavlou, Liang and Xue, 2007; Hann, Hui, Lee and Png, 2007; Malhotra, Kim and Agarwal, 2004; Wang, Lee, and Wang, 1998; Smith et al, 1996), trust and privacy relationships (Tang, Hu and Smith, 2008; Dinev, Bellotto, Hart, Russo, Serra, and Colautti, 2006; Hoffman, Novak and Peralta, 1999), and privacy policies (Mai, Menon and Sarkar, 2010; Hann, Hui, Lee and Png, 2007) are similar whether the context is online or in traditional organizations. However, new research topic areas such as the effects of privacy seals (Hui, Teo and Lee, 2007; Mai, Menon and Sarkar, 2010), privacy statements (Hui, Teo and Lee, 2007), personalization and privacy tradeoffs (Awad and Krishnan, 2006; Hann, Hui, Lee and Png, 2007) have also emerged as relevant research topics.

As a means to address the question as to why consumers are reluctant to participate in online activities, Pavlou et al. (2007) consider the implications of agency problems of adverse selection and moral hazard. They identified information privacy concern as an antecedent of perceived uncertainty in online buyer-seller relationships. Malhotra et al. (2004) addressed this same issue by drawing upon social contract theory to propose a theoretical framework of Internet users’ information privacy concerns. Hann et al. (2007) used expectancy theory in the context of motivated behavior to explore ways to mitigate individuals concern for privacy. Son and Kim (2008) considered individuals’ responses to information privacy threats online and classified
them into three categories: information provision, private action, and public action. Through their creation of a nomological network the authors were able to show how various customer responses are manifested in ways to protect the privacy of their information. They recommend that Organizations’ information practices give proper consideration to customers’ potential responses to such organizational practices (Son and Kim, 2008).

Trust is crucial in transactional, buyer-seller relationships, especially those containing an element of risk including interacting with web based systems (Reichheld and Schefter, 2000). Dinev et al. (2006) adapted Culnan and Armstrong’s (1999) privacy calculus model such that if the total effect of trust and control is higher total effect of privacy concerns and perceived risk, the user is likely to engage in a online transaction. Research has shown that trust between online business and its customers can be achieved by allowing the balance of power to shift towards a cooperative interaction environment (Hoffman and Novak, 1997). Wang et al. (1998) claim that a consumer-oriented information privacy model will lead to profitable business model for online transactions. In order to achieve a balance of power in online transactions online businesses need to recognize consumers’ rights to data ownership and offer opt-out or opt-in policies regarding information exchanges (Hoffman, Novak & Peralta, 1998). Tang et al., (2008) found that the ability to influence consumers’ beliefs about trusting online transactions is a result of how clearly they communicate their intention to protect customers’ privacy. The literature suggest several ways businesses can signal their intentions to protect customers’ privacy in online transactions these include posting
privacy statements, establishing privacy policies, and utilizing privacy seals.

Mai et al. (2010) found during their investigation of businesses using privacy seals that vendors’ websites with privacy seals could charge a premium the same products compared to vendors’ websites without a privacy seal. Hui et al. (2007) performed a study evaluating the effects of websites displaying a privacy statements or a privacy seal and found that displaying a privacy statement had significant effect on individuals disclosing their personal information where displaying privacy seals did not. Moores and Dhillon (2003) found that privacy seals increased customer confidence in the websites significantly. However online customers might be unduly placing trust in these websites because they unknowingly think these seals protect against fraud, which they do not. Organizations have the ability to actively manage the privacy concerns of Internet users by stating their privacy policy more prominently on their website because research has shown that privacy policies are valued by users (Hann et al. 2007).

Internet companies offer to personalize the online shopping experience for their customer as a means to build brand loyalty. The personalization process typically requires the customer to provide their personal and preference information such that the website can recall your information the next time you visit the site. Organizations who offer personalization need to consider the trade off customers make between their value for personalization and concern for privacy (Chellappa and Sin, 2005). A positive aspect of Web-based personalization for Internet companies is that it increases switching costs for it customers and serves as an important means of acquiring valuable customer information. A negative aspect is that customers may not value online personalization if
they have privacy concerns about providing the requested information. Chellappa and Sin (2005) found that a customer’s intent to use personalization services is positively influenced by their trust in the Internet Company they are doing business with. Awad and Krishnan (2006) examined the relationship between information transparency features and customer willingness to share information for online personalization. They found that customers who require information transparency are less willing to participate in personalization services. Internet organizations should accept the fact that the privacy sensitive consumers are unwilling to participate in personalization, despite additional privacy features and they should not overtly exhaust resources trying to get these customers to buy into the personalization process (Awad and Krishnan, 2006). Research has shown that it is important for online companies to understand and evaluate the values consumers have in the personalization and privacy relationship (Chellappa and Sin, 2005).

2.3.5 Location based privacy

The concept of personal privacy refers to keeping confidential those things an individual does not want known, such as a person's location (Solove, 2006). Ever since George Orwell penned the novel 1984, citizens of every free society has a fear that their government will track their every movement and invade their privacy with the use of technology. The development of new technologies such as GPS, mobile computing and Radio Frequency Identification (RFID) allows organizations the opportunity to collect evermore information about their customers (Pramatari and Theotokis, 2009). Location based services use these technologies to provide their customers with personalized
information however it may cost them their privacy because these technologies track their preferences, behaviors, and identity (Xu, Teo, Tan and Agarwal, 2009).

Research shows that information privacy concern affects the consumer attitude towards RFID-enabled services (Pramatari and Theotokis, 2009). A positive point about RFID technologies is that it allow companies to track products through the entire supply chain from the raw material phase to the point of sale to the end customer and possibly beyond. (Kapoor, Zhou and Piramuthu, 2009). This ability to track products through the supply chain allows for organizations to effective monitor their production processes and ultimately low their costs and to increase their profitability. However, the part of concern is the fact that organization (i.e. Apple) can still use some of these tracking technologies after they have sold the product to their customers and analyze information about their customers’ habits.

2.3.6 Cloud Privacy

Cloud computing is an evolving concept especially with the recent advancement of emerging technologies. Several researchers have tried to define cloud computing however there are no agreed upon definition. For the purpose of this study we will utilize the National Institute of Standards and Technology (NIST) definition of cloud computing which is as follows: “Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction” (Mell and Grance, 2009).

This proposed model of cloud computing promotes availability and
consists of the following five essential characteristics: on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service (Chen and Yoon, 2010). These characteristics allow the cloud to be utilized as the next utility service offering computing power instead of the traditional utility services of water, gas or power (Buyya, Yeo, Venugopal, Broberg, Brandic, 2009). This allows the cloud to offer scaled economic benefits to organizations by rationing computing resources and applications as needed. Three categories of cloud computing has emerged as a means of delivering cloud services. These three categories are, Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Each of these categories is designed to meet different customer needs. Examples of these services are products such as Google Docs (SaaS), Red Hat’s Openshift (PaaS), Amazon Web Services (IaaS). The main benefits to products like these is that they provide an opportunity to quickly and easily collaborate and access company data from anywhere with Internet access while saving money on capital expenditures by paying for resources being used. Web-based applications over the Internet, depicted by cloud, are quickly becoming standard starting applications for emerging technology companies (Chen and Yoon, 2010).

The dynamic nature of the cloud environment allows for services to be aggregated and changed dynamically by customers, and service providers can change the provisioning of services. There is the possibility that personal and sensitive data could be moved within an organization and/or across organizational boundaries without having the adequate controls in place to ensure compliance and protection of the information. Pearson and Charlesworth (2009) raises the concern “that the
speed and flexibility of adjustment to vendor offerings that benefits business and provides a strong motivation for the use of cloud computing might come at the cost of compromise to the safety of data.” One of these compromises seems to come at a cost to customer’s privacy. Privacy issues are not fundamentally caused by cloud computing, but are impacted by the exploitation of technology for economic benefit (Katzan 2010). For example Dhillon and Kolkowska (2011) note that essentially privacy in the cloud is an economic transaction and it depends on who is paying the bill. In most business models for the cloud, it is the advertisers who generates the majority of revenue for cloud providers therefore it is the interests of the advertisers that dictates how privacy issues are or are not resolved.

Privacy issues regarding risks within cloud environments are unique for various stakeholders (Pearson and Benameur, 2010). Privacy risks for individual users of cloud service exist such as exposure of personal information. These privacy issues are compounded when individuals are forced to give personal information against their will, or in a way in which they feel uncomfortable. Typically in these situations the organizations that are collecting the information fail to provide a legitimate reason to the customer as to why they need to collect their information (Tweney and Crane, 2007). For organizations using cloud services there is a privacy risk associated with non-compliance with internal privacy policies or external privacy regulations that cloud result in loss of reputation and credibility with their consumers. For cloud service providers the privacy risk is with the exposure of sensitive information being stored on their servers, non-compliance, legal liability, loss of reputation, and customer’s trust.

A lack of trust leads to a fear of confidential data leakage and loss of
privacy and this is a significant barrier to the adoption of cloud services is user fear (Pearson and Charlesworth, 2009). Research suggests that an organization’s integrity and accountability with respect to their information practices is important for easing privacy concerns and building user trust (Katzan, 2010). As a means to reduce cloud privacy risks, Pearson and Charlesworth (2009) recommend that organizations use a combination of privacy policies and contractual terms to create accountability in the form of transparent, enforceable commitments to responsible data handling. Transparency with respect to information handling practices allows individuals to be informed about how their data is handled within the cloud and defines the responsibility of people and the organization handling their personal information. Establishing accountability with privacy practices in the cloud helps to ensure compliance with cloud regulations and build trust.

The world privacy forum came up with a list of privacy issues for cloud computing most of which are concerned with the disclosure, jurisdiction, and legal aspects of information privacy (Gellman, 2009). They identified that the user’s privacy and confidentiality risks vary depending on the terms of service and privacy policies established by the cloud providers. As a user discloses information in the cloud their perception towards confidentiality, obligations and privacy rights change for select types of information or groups of users (Pearson and Charlesworth, 2009). Gellman (2009) noted that disclosure and remote storage might have adverse consequences for the legal status and protection of personal/business information. Another important cloud privacy issue stems from the fact that data and programs are stored off-premises and managed by a cloud service provider (Katzan 2010). The location of where the cloud
servers are located geographically while storing information in the cloud may have significant effects on the privacy and on the obligations of those who process or store the information (Pearson and Benameur, 2010; Zhou et al., 2010). In addition, conflicting issues may also arise because information in the cloud may have more than one legal location at the same time, with differing legal consequences (Gellman, 2009). Data ownership is also a privacy issue in cloud computing. These legal uncertainties may make it challenging to determine how to protect the privacy and confidentiality of users information in the cloud.

2.4 Discussion

The purpose of this chapter was to review the research literature in the values and privacy research domains and to identify research directions with regards to privacy in cloud computing. We examined the values literature along three levels of analysis; individuals, organizations and societal and noted that research on values is easily allows for a cross-level examination of the values construct. In essence the concept of values permeates across levels, society values influences individuals’ values and therefore also their behaviors and actions (Ravlin and Meglino, 1987; Agle and Caldwell, 1999). The research literature suggests that individuals’ values are an important aspect of their decision making process (Senger, 1971; Keeney, 1992). Through our review of the literature we identified Keeney’s (1992) Value Focused Thinking (VFT) approach of analyzing values in the decision making process as the best method for conducting our study on privacy values.

With respect to privacy researchers there is a general consensus that the concept of information privacy can be viewed, as the ability individuals to regulate
access to one’s personal information, such that it reduces vulnerability and unwanted disclosure. However, within context of emerging technologies, such as cloud computing, the concept of privacy is hard to gage. This is in part due to the cultural lag that exists between the development of emerging technologies and the norms within society associated with the use of the emerging technology. We found a limited amount of literature that had a research focus of understanding individuals’ values and the usage of cloud computing or information privacy in the cloud.

Research shows that cloud privacy is comprised of complex and comprehensive issues that need to be further studied, such that users and providers can proceed to utilize cloud technologies for mutual benefits. The contribution of this thesis is two-fold. First it establishes a value-based understanding of information privacy objectives for cloud computing. This will allow researchers to develop a richer understanding of privacy within the context of emerging technologies such as the cloud. Secondly, a cloud information privacy audit is developed based on the weighted importance of the identified cloud privacy objectives. These contributions allow organizations to be more proactive with their privacy practices instead of simply being reactive to external pressures.

2.5 Conclusion

There is a lack of clarity in organizations as to what individuals consider privacy to be. It is important to understand individual’s privacy values. Individuals seem to have divergent perspectives on the nature and scope of how their personal information is to be kept private in different modes of technologies. This study is concerned with identifying privacy objectives for protecting privacy in cloud computing environments.
We argue that in order to ensure privacy in the cloud we first have to identify individuals’ privacy objectives, which are imbedded in their values towards privacy. Therefore understanding and identifying individuals’ values with respect to privacy in cloud computing is important for the development of cloud privacy objectives and thus protecting privacy in the cloud.
Chapter 3 Theory and Research Design

3.1 Introduction

This chapter establishes the theoretical foundation for the design of this research study. In considering a research approach for a study it is important to understand the philosophical considerations associated with its application. Two philosophical perspectives, ontological and epistemological, need to be considered when selecting the research methodology to be used in a research study. The first consideration is the ontological perspective, which is based on the assumptions made about the nature of the social reality being investigated. The second consideration is the epistemological perspective, which are grounded in the assumptions made about the way in which knowledge of this reality can be obtained. In essence, the researchers stance towards as to what the ontological and epistemological assumptions should be in order to conduct rigorous research needs to be incorporated into the design of the research study.

In the social sciences, ontologies are concerned with discovering ‘what is the nature of social reality?’ Typically, most proposed theories about the nature of social reality are either categorized as idealist or realist (Blaikie, 2007). For the purpose of this study it is important to understand the idealist ontological view of the world. A researcher following an idealist ontology perspective views the world as representations of reality, which are a creation of individual minds. This implies that whatever we believe to be real is real only because we think it is real. Therefore, idealists believe reality is what we make it or construct it to be.

Epistemology is a theory of knowledge, of how human beings come to have
knowledge of the world around them. Basically it is how we know what we know. An epistemology provides a philosophical basis for the criteria from which one can decide knowledge to be adequate and legitimate (Crotty, 1998). This study is grounded in a constructionism perspective towards epistemology assumptions. Constructionists claim that knowledge is neither discovered from an external reality nor produced by reason independent of such a reality. They also argue that because humans cannot observe the world without using existing concepts, theories, background knowledge or past experiences it is impossible to make true discoveries about the world (Blaikie, 2007). Constructionists believe the activities involved in constructing knowledge occur in an environment of shared interpretations, practices and languages, which are deeply rooted in our history and culture. In short, as all social enquiries reflects the viewpoint of the researcher and all observations are theory-laden, therefore it is impossible to produce theory-free knowledge (Denzin and Lincoln, 2000).

These are philosophical assumptions that guide this study’s research design, which are discussed in greater detail in the sections below. The remainder of this chapter is organized as follows: Section 3.2 provides an introduction to the theoretical considerations for this study. Section 3.3 describes the research methodology to be used in this study. Section 3.4 outlines the research design for this study. Section 3.5 summarizes the contributions of this chapter.

3.2 Theoretical Concepts

This section discusses the theoretical concepts that support the research methods to be used in this study. In determining the methodological approaches for this study we considered the philosophical positioning discussed in the previous section.
order to ensure rigorous results the study has been completed in two sequential phases. The first phase utilizes value focused thinking as a methodological approach to extract individual privacy objectives from working professionals in the context of cloud computing. This is the research method used to answer the first research question of “what are the privacy objectives for cloud computing?” The second phase utilizes a design science approach for the development of a privacy audit framework for cloud computing. This is the method used for answering the research question of “how do you design a privacy audit for cloud privacy?” The theoretical concepts that support these research methodologies are now discussed in greater detail below.

3.2.1 Value Focused Thinking

Keeney (1992) indicated that there are two primary methods for thinking about decisions: alternative-focused thinking (AFT) and value-focused thinking (VFT). Historically, AFT is the more traditional decision-making technique of the two. AFT lists “identified” alternatives to make a decision from. This technique tends to limit the options to an existing set of alternatives, which often do not address the real issue of the problem. Whereas with VFT the decision maker first deciphers what is needed in the form of values and then generates a list of appropriate alternatives to address the real issue at hand. VFT tends to be more proactive in nature by developing a broader range of decision options for a specific problem context.

Keeney (1992) developed a systematic method to identify and organize values called the Value Focused Thinking (VFT) approach. The theory of values as discussed in the previous section provides the conceptual foundation for understanding
VFT. For the purpose of applying the VFT approach, values are defined as principles and used for evaluation by individuals (Keeney, 1992). Values that are of concern to the decision maker are made explicit by the identification of objectives. The VFT approach basically defines what decision makers’ care about by focusing on “what” is important and “how” to achieve it (Keeney, 1992). In order to do this VFT focuses on what the decision maker value in a certain context as a means to identify objectives for the decision problem. Keeney (1992) defined an objective as a statement of something one desires. Three features characterize an objective: a decision context, an object, and a direction of preference. From this process the fundamental objectives and means objectives are identified. Keeney (1992) describes fundamental objectives as “the ends that decision makers value in a specific context” and means objectives to be the “methods to achieve ends.” For this study the goal of using the VFT approach is to identify the fundamental and means privacy objectives in the context cloud computing. In order to achieve this there are a number of steps the researcher must follow.

The first step of applying the VFT approach is to identify and list personal values from each participant in the study. A description of the research problem and its contextual elements are shared with participants in the study who are then asked to express their concerns or issues relevant to the situation described to them. Typically, the researcher needs to be careful with respect to directly asking for the interviewee’s values because often times more latent values can easily be overlooked with this direct approach. One recommended interview technique to use is an in-depth interview where the researchers asks the interviewees “why is that important to you” questions about the problem context as a means to probe for more of underlying values of the
person being interviewed (Keeney, 1992). Dhillon and Torkzadeh (2006) suggest asking individuals to create a wish list, pose alternatives, and interpret consequences as a means to eliciting individual’s values.

The next step is to combine all the individuals’ values lists to form a comprehensive list of all values, there is bound to be some redundancy however this is not a concern since they may be some nuances derived from these redundancies as well. The goal of this process is to structure the values such that objectives can be created that accurately represent what an individual cares about in a specific situation. In order to convert these values into objectives, the researcher needs to transcribe them into a common form through techniques such as creating “wish lists” to help stimulate the identification of possible objectives (Keeney, 1992). Once all the values have been converted to objectives, duplicate objectives are removed and similar objectives are grouped together and form a primary objective which will later be classified as either a fundamental or means objective.

The researcher then separates objectives into fundamental and means objectives. Keeney (1992) suggested using the “Why is this Important?” test to separate means objectives from fundamental objectives and to establish their relationship. For each objective, asking “why is this important?” yields two types of possible responses. The first is that the objective is one of the essential reasons of interest in the situation and is fundamental for decision-making process. This is called a fundamental objective. The second response is that an objective is important because of its implication for some other objective(s). This objective is called a means objective. An important
step in the separation process is to repeatedly link objectives through means-ends relationships and specifying fundamental objectives (Dhillon and Torkzadeh, 2006). VFT not only uncovers the fundamental values and objectives that are usually hidden, but also provides a systematic way of identifying relationships among the objectives. The VFT approach provides an opportunity to gain a deep understanding of fundamental and means objectives for privacy within the context of cloud computing.

3.2.2 Design Science Concepts

The design science paradigm is grounded in engineering and sciences of the artificial (Simon, 1996). A design-science research study seeks to extend the boundaries of human and organizational capabilities by creating new and innovative artifacts (Hevner et al., 2004). These innovative artifacts provide intellectual and computational tools to improve organizational capabilities (Hevner, 2007). The goal of design science research is to solve relevant problems in a more effective and efficient manner. The importance of design science is well recognized in the IS literature (March and Smith, 1995; Hevner et al., 2004; Peffers et al., 2007; Iivari, 2007).

An important dichotomy must first be acknowledged before a true understanding or appreciation for design science can be realized. This dichotomy is that design is both a process and a product (Walls et al. 1992). Within the information systems research arena, processes and products are complexly integrated with each other, they are inseparable (Lee, 2000). In their seminal paper on design and natural science research on information technology March and Smith (1995) identified two design processes and four design artifacts produced by design research. The two processes identified are the
process of building and the process of evaluating. During the building process, design science researchers purposefully construct artifacts to address unsolved problems. These artifacts are then evaluated with respect to their ability to solve those problems. The four types of artifacts defined by March and Smith (1995) are constructs, models, methods and instantiations. These artifacts are intricately interlinked and contribute to and increase understanding of the problem domain and its solution. March and Smith (1995) stated that design research contributes to the field of IS research by addressing the kinds of problems faced by IS practitioners and providing them an implementable solutions that are both relevant and effective.

Zmud (1997) called for IS researchers to “further knowledge that aids in the productive application of information technology to human organizations and their management” and to cultivate and disseminate “knowledge concerning both the management of information technology and the use of information technology for managerial and organizational purposes (pg. #xxi).” Design science research has the potential to meet these demands by increasing the understanding of the problem domain while also improving the efficiency and performance of organizations through improved IS artifacts. Although this view of the design science research has not been well received by all of the IS research community. However, it is beginning to gain some traction in the IS research community with the works of March and Smith (1995), Hevner et al. (2004), Peffers et al. (2007) and livari (2007) who have helped to create a road map for fellow design-science researchers to follow. This roadmap is build upon the foundation that good design science research requires the researcher to incorporate a significant level of relevance, rigor and design into their research study.
The Relevance Cycle acts as an intermediary between the contextual environment of the problem domain and the design science activities of building and evaluating (Hevner, 2007). The relevance cycle gathers requirements from the environment and utilizes them to guide the research study. In addition, the relevance cycle also field-tests the research artifacts in the environment. The field-testing process will determine whether or not additional iterations of the relevance cycle are needed to meet the demands of the field. If additional iterations of the relevance cycle are required, feedback from the environment during the field-testing process will assist in refining the requirements being used in the research study.

The rigor cycle links the design science activities of building and evaluating the design artifact with the existing knowledge base of scientific theories and industry expertise that informs the direction of research project (Hevner, 2007). In design science studies the level of rigor associated with the project is contingent on the researchers ability to thoroughly research and reference the knowledge base to ensure the artifacts produced by the study are truly innovative to the field of study and its respective industry (Hevner et al. 2004). While theories can be sources that inspire creative ideas, Hevner (2007) warns that it may be restricting to the research field and thus the future knowledge base if we require that all design research be grounded on descriptive theories. Besides descriptive theories, the grounding of design science research can also be based on key identified opportunities/problems from the environment, existing artifacts or even creative insights (Csikszentmihalyi, 1996; Hevner et al., 2007). A good design science research study will contribute to both the environment and its informing knowledge base. The environment receives a new or improved artifact that
solves an important problem or takes advantage of a new opportunity. The knowledge base is expanded by any extensions to the original theories and methods made during the research, the new meta-artifacts (design products and processes), and all experiences gained from performing the research and field testing the artifact in the application environment (Hevner 2007).

The design cycle resides at the heart of any design science project. The core of this cycle is focused on the iteration process between the building of the design artifact, its evaluation, and its subsequent feedback to improve the design of the artifact. It is important for researchers to understand the dependencies of the design cycle on the other two cycles while maintaining its relative independence during the actual execution of the research project. During the design cycle the requirements or objectives are gathered from the relevance cycle while the theories and methods used to design and evaluated are drawn from the rigor cycle. During the execution of the design cycle a design-science researcher needs to maintain a balance between the efforts they spend building and evaluating the design artifact such that they can convincingly represent that both activities are based in relevance and rigor (Hevner, 2007).

While the guidelines and design science research framework developed by Hevner et al (2004; 2007) are good for assessing the quality of a design science research project they lack a defined process for conducting design science research (Peffers et al., 2008). To address this issue of a lack of a process for conducting design science research Peffers et al. (2008) developed the Design Science Research Methodology (DSRM). DSRM is a process model for conducting design science research (Peffers et al. 2008). The DSRM process model incorporates the following six steps: problem
identification and motivation, definition of the objectives for a solution, design and development, demonstration, evaluation, and communication. For the purpose of conducting this design-science research study we adopted a DSRM approach. The details of each of these steps will be discussed in detail in the research design section below.

3.3 Research Methodology and Design

A well-formulated research design will articulate the logical steps that link the empirical data from the study’s research questions to its conclusions (Yin, 2003). In essence it is a “blueprint” for the researcher to follow and address numerous problems including, what questions to study, what data are relevant, what data to collect, and how to analyze the results (Philliber, Schwab and Sloss, 1980). This research project will be performed in two phases. Phase one utilizes a value focus thinking approach to develop privacy objectives for Cloud computing and phase two utilizes a design-science approach to construct a privacy audit framework for ensuring privacy in Cloud computing. The remainder of this section will draft the design blueprints for both the value focus thinking approach and the design science approach to this study. The discussion on the design of the value focused thinking approach will focus on the data collection, data analysis, and evaluation aspects of the study. The discussion on the design science approach will focus on the applying Design Science Research Methodology (DSRM) to this study. As you will see in the following discussion the use of these two methods together are a natural fit because the results of the VFT phase can seamlessly integrate into the define objectives for a solution step of the DSRM process.
3.3.1 Argument and Research Questions

In order for cloud computing to achieve its full potential there should be a clear understanding of the various privacy issues, both from the perspectives of the service providers and the consumers of the technology. In the context of this study’s research strategy it is important to define a value proposition for personal information privacy in cloud computing environments. A value proposition will provide guidance to the researcher when analyzing individuals’ privacy values and thus inform the researcher as to individuals’ motives and desired actions regarding individuals’ privacy objectives in cloud computing. For this study the value proposition is defined as the net benefit or cost associated with gain or loss of personal information privacy when engaging in cloud computing.

The issue of ensuring cloud privacy is an important topic for organizations that have adopted cloud-based solutions within their organization. We argue that it is important to understand individuals’ privacy values with respect to cloud computing. This research argues that individual values are important in defining objectives for ensuring privacy in Cloud environments. Another challenge for management with respect to cloud privacy is that privacy in the cloud is an elusive concept. This is due to the evolving nature of the relationship between technology and privacy, which makes it difficult to determine privacy expectations within various technology usage, such as cloud computing. This challenge is compounded by a lack of clarity as to what organizations need to do in order to protect individuals’ privacy (Mason, 1986; Culnan and Williams, 2009). This is a result of not having well defined objectives for ensuring privacy. As noted in the previous section, this study uses Keeney’s (1992)
value focused thinking (VFT) approach to identify individual privacy values with respect to cloud computing technologies and to answer our the following research question:

What are privacy objectives for cloud computing?

We also argue that there is a need for organizations to develop socially responsible privacy practices. This view was also supported by Culnan and Williams (2009) who suggested that information privacy researchers need to focus on the following privacy management issues; how should an organization handle personal identifiable information, what are an organization’s responsibilities towards information privacy protection. Privacy managers or professionals are also concerned with similar questions such as how well does my organization manage information handling practices in the cloud? Or does my organization’s privacy practices meet required privacy regulations, Or what controls do we need to implement to meet the privacy expectations of my customers. Many of these types of questions can be answered for management by conducting an audit of their cloud privacy practices. We argue that it is important to develop a cloud privacy audit to ensure that organizations are being socially responsible with the information handling practices in cloud computing environments. As we noted in the previous section we will utilize a design science approach to a develop a privacy framework for ensuring cloud privacy and to answer the following research question:

How can an audit for cloud privacy be designed?

3.3.2 Research Design for the VFT Phase of the Study

For the data collection process 90 interviews were conducted with individuals with experience with cloud computing in one form or another. The research
subjects were a diverse mix of individuals working in different functional roles within various organizations with an average of 3-5 years of professional work experience. The interviewees consisted of 42% female and 58% male with an age range from 24 to 46 old. The interviews were conducted over a period of 8 months. The interviews were semi-structured in nature (see appendix A), which allowed for probing question techniques as recommended by Keeney (see Table 3.2) to extract the latent values of individuals with regards to their privacy values. The average duration for the interview was 40 minutes. Notes taken during the interviews were recorded in a master response document directly after the interview to ensure that all the richness of the interview was captured and documented.

Table 3.2 Techniques for Identifying Objectives reproduced from Keeney 1994 (pg. 35)

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>Develop a wish list.</strong> What do you want? What do you value? What should you want?</td>
</tr>
<tr>
<td>2</td>
<td><strong>Identify alternatives.</strong> What is a perfect alternative, a terrible alternative, some reasonable alternative? What is good or bad about each?</td>
</tr>
<tr>
<td>3</td>
<td><strong>Consider problems and shortcomings.</strong> What is wrong or right with your organization? What needs fixing?</td>
</tr>
<tr>
<td>4</td>
<td><strong>Predict consequences.</strong> What has occurred that was good or bad? What might occur that you care about?</td>
</tr>
<tr>
<td>5</td>
<td><strong>Identify goals, constraints and guidelines.</strong> What are your aspirations? What limitations are placed on you?</td>
</tr>
<tr>
<td>6</td>
<td><strong>Consider different perspectives.</strong> What would your competitor or your constituency be concerned about? At some time in the future, what would concern you?</td>
</tr>
<tr>
<td>7</td>
<td><strong>Determine strategic objectives.</strong> What are your ultimate objectives? What are your values that are absolutely fundamental?</td>
</tr>
</tbody>
</table>
8. **Determine generic objectives.** What objectives do you have for your customers, your employees, your shareholders, yourself? What environmental, social, economic, or health and safety objectives are important?

9. **Structure objectives.** Follow means-ends relationships: Why is that objective important? How can you achieve it? Be specific: What do you mean by this objective?

10. **Quantify objectives.** How would you measure achievement of this objective? Why is objective A three times as important as objective B?

### 3.3.2.1 Data Analysis for VFT Phase

For data analysis of the VFT phase, we used Kenney’s three step methodology to develop privacy objectives for cloud computing. The initial step of the data analysis process is to assemble a list of raw values from the interview process. This list will typically include items that are indicative of values but are not yet expressed as objectives such as alternatives, constraints, or criteria to evaluate objectives. These items will need to be converted into an objective before further analysis can be performed. It is important to note that an objective as defined by Keeney (1994) is a statement of something that one wants to strive towards. An objective is composed of three features: a decision context, an object, and a direction of preference (Keeney, 1994). For example one objective of privacy in cloud computing is to minimize third party access to personal information, the decision context is privacy in cloud computing, the object is third party access to personal information, and the direction of preference is less access rather than more. This process of converting alternatives, constraints and criteria into common form objective statements allows for the duplicates to be identified and removed from the master list of objectives (Dhillon and Torkzadeh, 2006; Keeney, 1994).
During the process of structuring values into objectives usually there are a number of sub-objectives dealing with a similar issue. These clusters of similar sub-objectives are grouped together to form a single objective and added to the list of objectives.

Just listing objectives offers very limited information to the decision maker or the researcher. To gain greater insight the objectives need to be compared with each other in the decision context. Keeney (1994) expressed that there are two types of objectives; fundamental objectives and means objectives. Keeney (1994) defines a fundamental objective as an objective that is concerned with the ends that a decision maker values in a specific decision context. While means objectives are methods to support the fundamental objectives. It is important to differentiate between the types of objectives by repeatedly linking objectives through means-ends relationships to identify fundamental objectives (Dhillon and Torkzadeh, 2006). In order to classify the objectives and to establish their relationship researchers ask the question of “Why is this objective important?” within the context of the decision problem (Keeney, 1994; Dhillon and Torkzadeh, 2006). There are two possible answers to this question. One is that it is essential to the decision context and therefore is considered to be a fundamental objective. The other answer is that it is important to the support of another objective and therefore it is considered to be a means objective. This process of performing a WITI test is repeated with each objective identified in a means-end link until a fundamental objective is identify. This process will separate the fundamental objectives from the means objectives and assist in identifying and classifying cloud privacy objectives.
3.3.2.2 Evaluation for VFT Phase

Once all the objectives have been sorted into either fundamental or means objective categories it is important to evaluate them to ensure their validity. Emory and Cooper (1991) noted that the validation process is unique for each study. While Keeney (1999) and Gregory and Keeney (1994) did not perform any validation procedures on the results from their VFT study, Torkzadeh & Dhillon (2006) considered content validity an to be an important step in their applications of the VFT methodology. There are many ways to ensure validity of the results of a research study. Typically the means of validation depends on the type of research methods being used. Dhillon and Torkzadeh (2006) used a panel of experts to validate the objectives derived from their VFT study as suggested by Emory and Cooper (1991). In order to validate the individuals’ privacy objectives identified in this study we decided to use a panel of experts as recommended by Dhillon and Torkzadeh (2006). The criteria used for selecting the panelists was that each of the members should either have an significant interest in the cloud privacy issues or have a job responsibility within the domain of auditing or utilizing cloud technologies. Based on these criteria a team of six information system security auditors was used to evaluate the analysis of the VFT phase. This panel of experts was used in both phases of this study. In the first phase they were used as a means to validate the cloud privacy objectives developed in the VFT phase of this study. During the second phase of this study this panel was assembled again as a confirmatory focus group to evaluate the effectiveness and applicability of the cloud privacy audit framework as a tool for ensuring cloud privacy. The details of this phase
will be presented in chapter 4 of this study.

### 3.3.3 Research Design for the Design Science Phase of the Study

The center of any design science project is the development process of the design artifact. The goal of this design science phase of the study is to develop a privacy audit framework for ensuring privacy in cloud computing environments. When conducting design science research the purpose is to design an artifact or incrementally improve the design, and evaluate its utility. (Hevner, 2004; March and Storey, 2008) In a design science research study we are addressing two complementary, yet different research goals, the first is to design an artifact and the second is to evaluate the artifact. Peffers et al. (2008) developed the Design Science Research Methodology (DSRM), an iterative process for conducting design science research. DSRM incorporates the following process steps, problem identification and motivation, definition of the objectives for a solution, design and development, demonstration, evaluation, and communication (see figure 3.1). In order to design a cloud privacy framework we adopted a DSRM approach. A six-step process mapping the design science phase of the study is present below Figure 3.1 DSRM model (Peffers et al., 2007, pg. 54)
3.3.3.1 Problem Identification and Motivation

The main purpose of this step is to define the specific research problem and value proposition of having a known solution to the problem (Peffers et al. 2008). A good design science research study starts by identifying a relevant IT problem and demonstrating that no adequate solutions already exist (March and Storey, 2008). The process of creating a problem definition statement allows the researcher to conceptualize the entire problem and its complexity (Peffers et al., 2008). Predetermining the value of the solution early in the research process creates buy-in amongst the stakeholders and motivates them to pursue a solution and it also helps to communicate the researcher’s understanding of the problem.

This study is concerned with the rapid advancements in cloud computing and the lack of ethical guidelines for its use. In particular, the increased value of information and amount of information being processed in the cloud has increased the risk of a loss of privacy. We posit that privacy is at risk due to a lack of ethical standards or best
practices to protect personal information in cloud computing environments. Developing an audit framework for auditing privacy practices in the cloud will reduce cloud users privacy risks.

3.3.3.2 Define Objectives for a Solution

The purpose of this step is to develop the objectives to be incorporated into the design artifact. The objectives should be inferred rationally from the research problem definition and knowledge of what is possible and feasible (Peffers et al., 2008). Given our problem statement that privacy is at risk due to a lack of ethical standards or best practices the objective of this phase of the study is to create an audit framework for ensuring cloud privacy. An important first step in the creation of audit requirements is the establishment of objectives for each auditing situation (Pathak, 2003). The importance of well-defined audit requirements is equivalent to the importance of gathering well define-system requirements for the development of new IT project. Hevner (2004; 2007) argues that in order to ensure that the designed artifact is relevant and useful the design requirements should be gathered from the contextual environment. The cloud privacy objectives developed in phase one of this study will be used as the cloud privacy audit requirement to initiate the design process of the cloud privacy audit framework.

3.3.3.3 Design and Development of Artifact

The purpose of this step is to create an artifact that provides a solution to the research problem (Peffers et al., 2008). Artifacts can be defined broadly as
constructs, models, methods, or instantiations (Hevner, 2004). They also include social innovations or new properties of technical, social, or informational resources (van Aken, 2004; Järvinen, 2007). An important resource required for design and development process is the knowledge of theory that is applicable to research objectives and problem can be in a giving context. Before any final artifact can be produced it is important that the design process goes though a series of iterations or cycles. Each cycle begins with the building of a design artifact, which is then evaluated, and then the feedback from the evaluation is used to make improvements to the design of the artifact. Tremblay et al. (2010) state that this design-evaluate iterative process should continue until nothing new is learned. Determining when “nothing new” is being learned is a challenging undertaking by itself. This is because there is always room for improvement and there is a fair amount of subjectivity in determining when the design of an artifact is indeed complete. At some point in time the researcher has to choose to satisfice in order to move forward.

In this step we utilized focus groups during the design and evaluation process as recommended by Tremblay et al. (2010). Stewart et al. (2007) define a focus group as a moderated discussion among 6–12 people who discuss a topic under the direction of a moderator. Focus groups can be utilized for multiple purposes throughout the design science research process. In particular the use of two types of focus groups are used to achieve different research goals; (1) exploratory focus groups (EFGs) (2) confirmatory focus groups (CFGs) (Stewart et al., 2007; Tremblay et al., 2010). EFGs are useful when little is known about the phenomenon to achieve incremental improvements in artifact
design (Tremblay et al., 2010). CFGs are used to demonstrate the utility of the artifact design in a field-testing environment (Tremblay et al., 2010). The use of CFGs in this study will be discussed in greater detail in step 5 where as the use of EFGs are discussed next.

The use of exploratory focus groups improves the design process by bringing a group of content experts together and using their specific expertise to evaluate of the design artifact and propose improvements to the design artifact. In essence the primary goal of EFGs is to provide feedback on the design artifact that can be utilized for design changes. Receiving feedback for the improvement of the design artifact is a vital component of design science research (Markus et al., 2002). An iterative process cycle of building and evaluating of the artifact is continued until the artifact is released for field-testing in the contextual environment.

It is important to note that the identification process of focus group participants is not as statistically rigorous as it is for survey-based research (Tremblay et al., 2010). Focus group participants should be selected based on their characteristics in relation to the topic that is being discussed (Stewart et al., 2007). Tremblay et al. (2010) recommend that for design science research study the participants should be from a population familiar with the problem domain for which the artifact is designed so they can adequately contribute to the artifact evaluation and refinement process. When assembling an EFG for a design science study besides looking for participant with specific characteristics that relate to the problem domain it is also important to consider the size of the group. Morgan (1998) claimed that the dynamics of smaller
groups require greater participation from each member and therefore suggested a boundary of 4 to 12 participants.

During the identification process of the EFG for this study we determined that it was important that each participant had adequate experience addressing privacy issues from an IT, legal or regulatory perspective. In addition, we were looking for individuals who have been involved with the process of accessing or implementing some form of cloud computing technology. We selected the following six individuals to participate in the EFG for this design science study.

- 1\textsuperscript{st} panelist is a Field Service Engineer with 8 years of IT experience and has recently been involved in providing managerial and solutions to the Federal government in the realm of biometrics, identity management and IT security.
- 2\textsuperscript{nd} panelist is an attorney with 15 years experience in Internet law with a focus on privacy law and compliance. He is also a Certified Information Privacy Professional.
- 3\textsuperscript{rd} panelist is an Information Security Officer at a large public university with 11 years experience in IT management.
- 4\textsuperscript{th} panelist is a programmer analyst for a national healthcare provider with 10 years experience in the IT industry.
- 5\textsuperscript{th} panelist is a Technology Advisor for a large national bank with 28 years of IT experience. He has an expertise in designing complex information security architectures.
• 6th panelist is a senior IT consultant with 26 years of experience in the IT field. He is a certified Project Management Professional and has been the lead on both public and private sector IT projects.

3.3.3.4 Demonstration of Design Artifact

The purpose of this step is to demonstrate the use of the design artifact to solve one or more instances of the problem (Eekels and Roozenburg 1991; Nunamaker et al., 1991; Peffers et al. 2008). A demonstration of the artifact can vary from a single act of demonstration (Van Aken, 2005) to prove that the idea works, to a more structured evaluation process (Hevner et al, 2004) of the developed artifact. The application of the design artifact in experimentation, simulation, case study, proof, or other appropriate activity is sufficient to qualify as a demonstration. It is important that effective knowledge of how to use the artifact to solve the problem is utilized during the demonstration process. In order to ensure proper application of the cloud privacy audit framework we utilized an audit team of information system security professions to develop a cloud privacy audit program with a simulated cloud environment.

3.3.3.5 Evaluation of Design Artifact

The purpose of this step is to observe and assess how well the design artifact supports a solution to the defined research problem (Peffers et al., 2008). An evaluation process determines if the results from use of the design artifact in the demonstration phase meet the objectives for the solution as defined in step two. For design science research, evaluation methods can take many quantitative or qualitative forms.
and such experimentation, case study, action research, which incorporate satisfaction
surveys, client feedback, or simulations (Peffers et al. 2008, Hevner, et al., 2004;
Vaishnavi and Kuechler, 2008). Conceptually, such evaluation could include any
appropriate empirical evidence or logical proof. It would be best if the designed artifact
could be applied in a real business setting to assess its impact and utility directly, such as
using an action research method (Zheng, 2009). However, several issues prevent this
type of full-scale evaluation for this dissertation. First, it is difficult to find the right
organization that has the need for a cloud privacy audit and is willing to fully
cooperative in applying the cloud privacy audit framework. Second the length of time
required to perform a complete audit from beginning to end is rather extensive. Thus, it
is impractical to conduct a full-scale evaluation of the Cloud Privacy Audit Framework
during a live audit process for this dissertation.

Therefore, instead of directly measuring the utility and ease-of-use of the
designed artifact, we collected evidence from auditors’ perceptions of the cloud privacy
audit framework. Our evaluation objectives are to evaluate the Perceived Usefulness
and the Perceived Ease-of-Use of the artifact. Table 3.3 illustrates the major objectives
of the evaluation and some examples of expected evidence from auditors’ feedback. We
collected qualitative data mainly through group discussions with a confirmatory focus
group consisting of a team of six information system security auditors. Utilizing
qualitative data may provide a deeper understanding and insights about the research
domain (Baskerville et al., 2007). Which in turn, provides us with more effective
information to improve the design artifact in the next design cycle. At the end of the
evaluation process a decision needs to be made to either go through another iterate of
design and evaluate or if the design artifact is sufficient enough to be consider a valid
solution to the research problem. This evaluation approach is suitable to the designed
artifact because the approach is human centered and it needs humans to interact
intensively with the framework.

Table 3.3 Evaluation objectives

<table>
<thead>
<tr>
<th>Evaluation Objectives</th>
<th>Expected sample evidence from qualitative data analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Perceived Usefulness</strong></td>
<td>Users think the artifact is useful to the audit planning process and for adapting existing audit programs to cloud environments.</td>
</tr>
<tr>
<td></td>
<td>• The framework offers a good insight into the cloud privacy risks that need to be monitored.</td>
</tr>
<tr>
<td></td>
<td>• The framework provides a good foundation to assess privacy controls.</td>
</tr>
<tr>
<td><strong>Perceived Ease of Use</strong></td>
<td>Users think the framework is easy to understand and implement.</td>
</tr>
<tr>
<td></td>
<td>• The framework is easy to adapt to our audit planning process</td>
</tr>
<tr>
<td></td>
<td>• The framework is easy to understand.</td>
</tr>
</tbody>
</table>

For the purpose of this step we utilized a confirmatory focus group (CFG) to
evaluate the design artifact. CFGs are a good way to evaluate the utility of the artifact
design in the contextual environment (Tremblay et al., 2010). Stewart et al. (2007)
identified the following four reasons as to why focus groups are an appropriate for
evaluation of design science research studies.

- Flexibility: Focus groups allow for an open format and are flexible enough to handle a wide range of design topics and domains.
• Direct Interaction with Respondents: This allows for the researcher to clarify any questions about the design artifact as well as probing the respondents on certain key design issues.

• Large Amounts of Rich Data: The rich data allow deeper understandings, not only on the respondents’ reaction and use of the artifact but also on other issues that may be present in a business environment that would impact the design.

• Building on Other Respondent’s Comments: The group setting allows for the emergence of ideas or opinions that are not usually uncovered in individual interviews. Additionally, causes of disagreement can point to possible problem areas with the proposed artifact.

The identification process of participants in the CFG for the evaluation process of this design science study was similar to the identification process of EFG. Many of the same attributes were considered to be also of value to the evaluation process such as having adequate experience addressing privacy issues from and IT, legal or regulatory perspective and being knowledgeable in cloud computing technologies. There was one important aspect of the participant selection process that was different and that was a desire to utilize a pre-existing group. The rational for using pre-existing groups for design science studies is that there may be some advantages to doing so because the group participants already have worked together and the focus group may approximate a realistic environment (Kitzinger, 1994). Therefore we identified and selected an existing audit team with six members to participate in the CFG for this study.

3.3.3.6 Communication of the Design Science Study

The purpose of this step is to communicate the importance of the research problem, the artifact as an innovative solution to the problem, the rigor of its design process, and the effectiveness of the artifact to researchers and practitioners.
The reporting of the results in this study aims to follow King’s (1998) recommendation for reporting qualitative results in that the researchers should create an account structured around the main themes identified, drawing illustrative examples from transcripts as required. Tremblay et al., (2010) also provide some useful guidance as to how focus group results should be reported. They recommend that “Short quotes are used to aid in the specific points of interpretation and longer passages of quotation are used to give a flavor of the original discussions” (Tremblay et al., 2010). The results of this design science study are communicated in this dissertation. In addition sections of this dissertation will be craved out for publications in scholarly research journals.

3.4 Conclusion

This chapter established the theoretical foundation for the design of this research study. It position the research along an idealist and constructionist view of the world, where the researcher believes that reality is what we make it or construct it to be. These theoretical perspectives were used to select two research methods, Value Focused Thinking and Design Science Research Methodology, that would best answer our research questions. The rational for using these methods in the research study was given along with the research design for the two phases of this study. Phase 1 utilizes a value focused thinking approach and will be covered in chapter 4. Phase 2 utilizes a Design Science Research Methodology and will be presented in chapter 5. The design of the research study was provided such as to clarify the procedures to be used during each phase of the study. The research approaches presented in this chapter are justified based on the nature of the research problem and the theoretical perspective adopted by the
researcher.
Chapter 4 Privacy Objectives for Cloud Computing

4.1 Introduction

The purpose of this chapter is to present the fundamental and means objectives for ensuring privacy in cloud computing. The privacy objectives presented here are the results of the first phase of our study. The initial phase of this study utilized a value focused thinking approach to develop objectives for ensuring privacy in cloud computing. In the following sections we present a detailed data analysis and discussion of the cloud privacy objectives identified in this study. The discussion will focus on the importance of the derived objectives with respect to the extent literature and provide a platform from which to establish their relevance and contributions to overall strategic objective of ensuring privacy in cloud computing. The concluding section of this chapter discusses the importance of ensuring privacy in the cloud and identifies a need for a privacy audit framework, which is subsequently presented in the following chapter.

4.2 Making Values Explicit

The research community has long recognized the need to clarify values as a means to develop organizational strategies. Selznick (1957) noted that sound organizational leadership requires “proper ordering of human affairs, including the establishment of social order, the determination of public interest and the defense of critical values.” In order for an organization to achieve a level of excellence, Peters and Waterman (1982) propose that they need to figure out their “value system”. This line of reasoning is supported by Keeney’s (1994) claim that values define all that you care about in a specific decision context and that they act as guiding principles for evaluating
the desirability of any possible alternative or consequences. The process of thinking about values forms the basis for quality decision making by: creating alternatives, identifying decision opportunities, guiding strategic thinking, interconnecting decisions, guiding information collection, facilitating involvement in multiple-stakeholder decisions, improving communication, evaluating alternatives, and uncovering hidden objectives (Keeney 1994).

The process of identifying values is clarified with an explicit statement of specific objectives. An objective is a statement of something that one wants to strive towards and consists of three features: a decision context, an object, and a direction of preference. Keeney (1994) noted that the process of interviewing research subjects will typically generate an initial list of raw items, however these items are not solely expressed as objectives. The process of identifying and structuring objectives is a difficult task and the relation between the objectives is easily misconstrued, leading to an unclear understanding of the relationships among objectives. Having clear and well-defined objectives is important to fully understanding problem domain and the contextual aspects of the decision to be made.

4.3 Data Analysis

For the purpose of classifying objectives we use the method applied by Dhillon and Torkzadeh (2006) and define objectives at two levels. In order to simplify the organization process of objectives Dhillon and Torkzadeh (2006) restating values in a common form structure. Converting the raw values items into common form objective statements allowed for the duplicates to be identified and removed from the list of sub-objectives. The next step is to classify these newly formed “sub-objectives.”
During this process a number of similar sub-objectives dealing with the same issue are identified. These similar sub-objectives were grouped together to form a single sub-objective. Because of the size of the list of raw values gathered in our study, this step was performed in multiple iterations. The first iteration reduced the list of raw values down to 217 common form objectives and the second iteration resulted in our final list of 105 sub-objectives.

In the final step of this process, these sub-objectives are clustered together based on similar themes. During this step, we analyzed the 105 sub-objectives and clustered similar objectives together forming 23 main objectives. These clusters form main objectives, which are classified as either a fundamental, or means objective. These objectives were then compared with each other in order to gain further insight in the context of ensuring privacy in cloud computing environments. As noted in earlier chapters it important to differentiate between the types of objectives by repeatedly linking objectives through means-ends relationships. This is known as performing a “why is this important” (WITI) test. The result of this type of testing is a better understanding of the directional relations between the objectives. In essence there are only two possible outcomes to a WITI test. One is that it is essential to the decision context and therefore is considered to be a fundamental objective. The other answer is that it is important to the support of another objective or a fundamental objective and therefore it is considered to be a means objective. This process was repeated until all the main objectives were separated into fundamental objectives or means objectives. Initially this process resulted in 7 fundamental objectives and 16 means objectives.
4.4 Results

The results will be presented in two distinct sections. First we will discuss, in detail, the six fundamental objectives for ensuring privacy in cloud computing, that were derived from the value focus-thinking phase of this study. These fundamental objectives are as follows: (1) to increase trust with cloud provider, (2) to maximize identity management controls, (3) to maximize responsibility of information stewardship, (4) to maximize individual’s understanding of cloud service functionality, (5) to maximize protection of rights to privacy, (6) to maintain the integrity of data. Secondly, we will discuss in detail the 19 means objectives identified in this study. This process will include a discussion on the importance of the fundamental or mean objective as it relates to ensuring cloud computing. It will also provide a bridge from the data collected in our interview process and the established literature as a means to build a solid foundation for the justification of the objective being discussed.

Table 4.1 Fundamental Objectives

<table>
<thead>
<tr>
<th>F.O. #1: To increase trust with cloud provider</th>
<th>F.O. #2: Maximize identity management controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure future access to my information by selecting a service provider who has a stable future.</td>
<td>Limit the amount of personal information I provide to organizations using cloud services.</td>
</tr>
<tr>
<td>Identify a cloud service provider who has a stable future.</td>
<td>Limit the amount of personal information in the cloud.</td>
</tr>
<tr>
<td>To find a cloud service provider who I can trust with my personal information.</td>
<td>To be informed about the privacy status of my personal information.</td>
</tr>
<tr>
<td>To identify a stable company I can trust with my personal information.</td>
<td>To ensure that my anonymity is protected.</td>
</tr>
<tr>
<td>To minimize the amount of personal information provided to cloud providers I do not trust.</td>
<td>To ensure the protection of personal information through third party validation.</td>
</tr>
<tr>
<td>To use a reputable cloud service provider.</td>
<td>To know where my personal information is being stored.</td>
</tr>
<tr>
<td>To utilize a cloud service provider with a positive reputation.</td>
<td>To maximize control of identity</td>
</tr>
<tr>
<td></td>
<td>To maximize the protection of my personal identity.</td>
</tr>
<tr>
<td></td>
<td>To protect my reputation.</td>
</tr>
<tr>
<td>F.O. #3: Maximize responsibility of data stewardship</td>
<td>F.O. #4: Maximize individual’s understanding of cloud service functionality</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>---------------------------------------------------------------------</td>
</tr>
<tr>
<td>To ensure that cloud service providers consider being data custodians as an important aspect of their service. To increase awareness towards responsibility of protecting data / information.</td>
<td>To ensure understanding of current technology advancements. To maximize understand the controls available to protect my personal information. To maximize the awareness of increasing the capacity of the system. To increase the methods available to gain access to information stored in the cloud.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>F.O. #5: To maximize protection of rights to privacy</th>
<th>F.O. #6: To maintain the integrity of data</th>
</tr>
</thead>
<tbody>
<tr>
<td>To ensure that my cloud service provider respects my rights for privacy. To ensure that the cloud service provider follows local privacy laws. To have standard international privacy laws for the cloud. To identify cloud service providers who have not had any legal issues. To protect my privacy rights with a legal contract.</td>
<td>Ensure that my cloud service provider uses encryption tools to protect my information. To minimize the risk of having my personal data corrupted. To protect the integrity of my personal data.</td>
</tr>
</tbody>
</table>

**Table 4.2 Means Objectives**

<table>
<thead>
<tr>
<th>M.O. #1: To maximize effectiveness of secure data transfers</th>
<th>M.O. #2: To optimize ease of use of cloud technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>To maximize efficiencies for data transfers between systems. To maximize time efficiency with respect to data transfers. Utilize encryption to protect my information while the data is in transit.</td>
<td>To maximize the convenience of accessing my information in the cloud. To minimize the challenges of using cloud technologies.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>M.O. #3: To maximize technology infrastructure competencies</th>
<th>M.O. #4: To minimize unnecessary access to information</th>
</tr>
</thead>
<tbody>
<tr>
<td>To ensure technical security measures are being used to protect my personal information. To ensure that the latest technology and software are utilized to protect my information. To ensure the physical security of the technology infrastructure housing my personal information. To maximize the security of the cloud's IT infrastructure. To provide a secure environment for collaboration with others.</td>
<td>To ensure that I know who I am giving my personal information to. To ensure that only people I authorize have access to my personal information. To limit my cloud service provider's access to my information to those who absolutely need access. To maximize control over who can access my personal information. To monitor my profile accounts to ensure access to my personal information is granted only to those I authorize to have it.</td>
</tr>
<tr>
<td>M.O. #5: Increase Standardization of cloud technologies</td>
<td>M.O. #6: To optimize the effectiveness of privacy policy governance</td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>To ensure privacy regulations stay current with the capabilities of emerging technologies.</td>
<td>Ensure that the cloud service provider has similar privacy values that I have.</td>
</tr>
<tr>
<td>To ensure protection of personal information in the cloud through regulation and industry design standards.</td>
<td>To ensure that the cloud service provider has high ethical standards.</td>
</tr>
<tr>
<td>To ensure that I have the ability to change service providers when I choose to do so.</td>
<td>To minimize changes to privacy policy agreements.</td>
</tr>
<tr>
<td></td>
<td>To minimize misunderstandings with respect to cloud provider's privacy policy.</td>
</tr>
<tr>
<td></td>
<td>To minimize the possibility of privacy or security breaches.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>M.O. #7: To maximize performance of vulnerability assessments</th>
<th>M.O. #8: To increase control over information disclosure</th>
</tr>
</thead>
<tbody>
<tr>
<td>To maximize the understanding the risk involved with using a cloud service provider.</td>
<td>Limit the amount of information I disclose in the cloud</td>
</tr>
<tr>
<td>To minimize privacy/security risks while maximize benefits of cloud services.</td>
<td>Limit the disclosure of information that can personally identify me.</td>
</tr>
<tr>
<td>To minimize risk of using the cloud services.</td>
<td>To minimize the disclosure of personal information.</td>
</tr>
<tr>
<td>To perform a risk assessment of privacy breaches before using the cloud.</td>
<td>To be properly notified when there is a privacy/security breaches.</td>
</tr>
<tr>
<td>To perform a risk assessment of using the cloud service.</td>
<td>To increase ability to manage disclosure of personal information.</td>
</tr>
<tr>
<td>To protect my information from hackers.</td>
<td></td>
</tr>
<tr>
<td>To reduce the like likelihood of hackers gaining access to my information.</td>
<td></td>
</tr>
<tr>
<td>To reduce the risk of privacy breaches.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>M.O. #9: To ensure CSP has effective HR practices</th>
<th>M.O. #10: To minimize government access to information</th>
</tr>
</thead>
<tbody>
<tr>
<td>To ensure the cloud service provider has a strict hiring process of employees.</td>
<td>To limit the control governments have over access to my personal information.</td>
</tr>
<tr>
<td>To ensure that the cloud service provider has a proper security/privacy training program for their employees.</td>
<td>To reduce the governments ability to seize my information.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>M.O. #11: To maximize effectiveness of independent oversight of privacy practices</th>
<th>M.O. #12: To optimize access controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>To audit the cloud service provider to ensure they are following their privacy policy.</td>
<td>To ensure that my passwords are well protected and secure.</td>
</tr>
<tr>
<td>To audit the cloud service provider to ensure they are following their privacy regulations.</td>
<td>To ensure the authentication process is efficient and secure.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>M.O. #13: To optimize segregation of information</th>
<th>M.O. #14: Minimize third party access to information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Segregate information about myself into specific identity groupings such as personal, family, friends, professional, academic.</td>
<td>To ensure that my cloud service provider does not share my information with a third party.</td>
</tr>
<tr>
<td>To ensure that my personal information is compartmentalized within the server based on who needs to view the information.</td>
<td>To limit the collection of my information collected by my cloud service provide or third party.</td>
</tr>
<tr>
<td>To ensure confidential information is separated and protected at higher levels of confidentiality.</td>
<td>To limit third parties from accessing my personal information.</td>
</tr>
</tbody>
</table>
### M.O. #15: To minimize liability concerns
To ensure that my data is removed from the cloud server when I terminate my service agreement.
To ensure that my personal information is stored in a safe legal jurisdiction.
To hold cloud service providers legally liable for privacy/security breaches.
To reduce my legal responsibility/risk.

### M.O. #16: To ensure provider has effective internal controls
To ensure internal controls are established to protect my information.
To ensure the cloud service provider has good monitoring practices of their infrastructure.
To protect my information through well defined internal controls and procedures.

### M.O. #17: To maximize availability of cloud resources
To ensure the accessibility to my personal information in the cloud.
To maximize the availability of information when needed.
To maximize the availability of the cloud services.
To maximize the availability of the internet connection to my information.
To maximize the reliability of cloud services.
To ensure access to personal information at a future date through reliable data backups.

### M.O. #18: Increase awareness of data ownership
To clearly define who owns the data stored in the cloud.
To maintain intellectual property rights to my information.

### M.O. #19: To ensure service level agreement meets privacy requirements
To ensure contracts with vendors guarantee that we will receive the data back after the expiration of the contract.
To ensure contracts with my cloud service provider express the legality of the information once it is in the cloud’s possession.
To ensure contracts with vendors guarantee we own our own data.
To ensure CSP SLA meet it privacy requirements or industry standards which ever are more stringent.

### 4.4.1 Fundamental Objectives for Cloud Privacy

#### 4.4.1.1 Increase Trust with Cloud Provider

A user of cloud services needs to be able to trust that the cloud service provider will respect and protect their privacy. Trust with the cloud provider is the degree to which one party will rely on the assertions or information provided by another. Without the ability for a cloud user to rely on the information and services from a cloud service provider, there is likely to be limited adoption of cloud services. Basically, the lack of
trust leads to under utilization of cloud technologies. In essence people, businesses, and organizations tend to classify data into different types of categories and each type of data or information classification has a trust level associated with it. Before a party is willing to share or grant access to a specific type of information they require a certain level of trust be established, and each data type or information classification could have its own trust requirements. For example if a user only has a minimal degree of trust in a cloud provider to protect their privacy, they may only use the cloud service as a means to store non-sensitive or non-critical information. This implies that the cloud for those who do not trust it will only be used as a data warehouse for non-sensitive information and not for other computing functions such as key operational analysis or running strategic applications. Therefore the full benefit of cloud computing is not achieved because individuals do not trust the cloud provider to protect the privacy of their information.

Establishing a trusting relationship between the cloud service providers and consumers of these shared services should be a primary goal in the development of the cloud, One individual we interviewed expressed concern for the loss of control of information with respect to protecting his privacy. He stated the following:

“I am concerned about the loss of control of information, and I am not just talking about confidentiality, which for many applications is more than enough to reject this new concept, I am talking about an absolute loss of control, in fact, I cannot control if the provider of services in the cloud uses our information, sells it, changes it, or deletes it. This also means that there is a strong possibility of a loss of data integrity. These facts make me feel slightly reluctant to trust cloud computing services.”

The following statement captures another example of the importance of the cloud provider’s trustiness provided by an interviewee,
“I believe most individuals would like to work and deal with people or organization that they trust. No one wants to put his or her personal information or any other assets for that matter in the cloud if they do not trust the cloud provider. To do so, people need to know how their information in the cloud will be treated, at which degree their privacy can be trusted therein.”

This notion that trust in the cloud provider is important for ensuring privacy in cloud computing is also supported by a statement made by one of the information systems auditors who during the validation process stated the following,

“People trust more when they understand the systems they are using better. Therefore, cloud service providers should clearly communicate how the cloud technology is configured and what controls they have in place to protect the users information and privacy.”

The relation between trust and privacy is an important topic that has been examined in the information systems literature from many different perspectives. Wang, Lee and Wang, (1998) reported that the most critical issue identified by Internet customers is a fear and distrust regarding loss of personal privacy in the electronic commerce markets. Researchers adopting a social exchange theory view towards trusts suggest that it is the most important asset from which businesses are built upon (Luo, 2002; Benassi 1999; Zucker, 1986). Within the realm of the Internet understanding the nature and antecedents of trust has been identified as a major issue for both researchers and practitioners (McKnight et al., 2002). Luo (2002) suggests that increasing customers’ trust online is a solution to online related privacy concerns.

Other researchers such as Campbell (1999) and Gengler and Leszczyc (1997) have also considered increasing trust a means to manage consumer privacy concerns. Institution-based trust mechanisms have been proposed as a possible solution to solve privacy concerns (Luo, 2002; McKnight et al., 2002). Institution-based trust
is the belief that needed structural conditions is present to enhance the probability of achieving a successful outcome (McKnight, Choudhury, and Kacmar, 2002). McKnight et al. (2002) argue that trust makes consumers comfortable sharing personal information. McGraw (2002) noted that if customers trust that personal and transactional information remains private they would flock to e-commerce in droves. Privacy and trust issues have been considered a major deterrent to the adoption of cloud computing (Pearson and Benameur, 2010; Buyya, Pandey and Vecchiola, 2009; Jaeger, Lin and Grimes, 2008).

Trust is developed through the cloud provider’s ability to apply privacy policy controls and to guarantee that access controls within policies are being adhered to. Pearson and Charlesworth (2009) proposed that there is a need to increase accountability in the cloud provider as a means for protecting privacy in the cloud. In their argument they claim that cloud providers transparency towards their handling of personal identifying information that permits meaningful accountability should be emphasized because it augments user’s trust and thus his/her conviction to use that cloud provider (Pearson and Charlesworth, 2009).

4.4.1.2 Maximize Identity Management Controls

The evolution of cloud computing has resulted in an amalgamation of various technologies as a means to meet the demands of a cluster of interdependent software and services. This complexity within cloud environments necessitates stronger identity management controls (Gopalakrishman, 2009). Identity management has been broadly defined as the management of digital identities or personal identifying data (Halperin and Backhouse, 2008). In the dynamic environment of cloud computing, controls need to be established to protect and ensure the entire lifecycle of user identities.
and their associated credentials and entitlements (Gopalakrishman, 2009). Without better controls for managing identities, we will continue to struggle with issues such as identity theft, spam, malware, and cyber fraud and we will be unable to ensure individual users that their privacy is protected (Cavoukian, 2009). IS researchers have suggested that technical controls such as digital signatures for nonrepudiation, cryptography strategies for encrypting databases and data transfers or federated identity management systems as the best solutions for managing individual’s identities in a cloud environment (Yan, Rong, Zhao, 2009; Jensen, et al. 2009). However, it is also important that organizations understand that the importance of including the user into the identity management process. Cavoukian (2009) argued that users must be empowered to execute effective controls over their personal information. Users need to able to determine what information is being shared with which parties and for what reason. Ultimately, users need to be able to evaluate the trustworthiness of a cloud service provider with regards to information handling practices and understand the consequences of sharing their information with them.

In this study individuals expressed concerns over the protection of their personal identity. In one case an individual proclaimed, "I am pretty cautious with my identity. I don’t care to share personal information on social networking sites and don’t use them at all. I try to be fairly careful about releasing my credit card info when buying things online. I will only give out personal info to someone I know or have reason to believe legitimately requires it.”

Another participant in the study claimed that, "My own identity has a great value to me. I always look for a way to secure my personal
information. I am wary of scams or spams asking for your personal information so when giving out my information, I always check for the credential of the receivers.”

A third participant stated,

“I enjoy my privacy. However, I understand that in order to accomplish many of my goals, I necessarily have to offer up some of my personal information. I strongly believe that everyone should have a healthy mistrust of those in a position of power or authority. This doesn’t mean that I don’t respect authority as a system. I simply feel that its practitioners should not be given the benefit of the doubt. It is every citizen’s duty to hold Governments, Corporations, and other individuals accountable”.

An underlying theme within these statements is that while individuals understand the necessity of providing certain personal information in order to gain access to cloud services they are wary of the potential for lack of controls or ethical standards on behalf of the cloud provider. Other concerns regarding the protection of personal identifying information also emerged in the study such as ensuring the protection of an individual’s right to anonymity, being informed when personal identifying information has been breached. Researchers argue that there is a strong need for an efficient and effective privacy-preserving system for managing personal identifying information (Angin et al., 2010). Identity management has been identified as one of the core components for ensuring cloud privacy and security.

4.4.1.3 Maximize Responsibility of Information Stewardship

While notion of information stewardship is nothing new in the domain of information privacy, recent events such as data breaches at Zappos, Linked-in or Sony have reinforced the importance of good information stewardship. Pym and Sadler (2010) defined good information stewardship as the ability to understand how information
flows between the components of a system. With cloud computing this understanding is more challenging given their highly distributed complex systems. In the context of information privacy, information stewardship is a management approach concerned with protecting information that can identify individuals. This concept of information stewardship is intended to convey a fiduciary level of responsibility toward data management practices (Rosenbaum, 2010).

Straub and Collins (1990) recognized the importance of personal data being carefully stewarded throughout its organizational life. They identified four stages of good stewardship. The first stage begins with only collecting information that is absolutely required. Secondly, individuals need to be informed and provide consent as to what information is being collected and its intended usage. While the personal information is maintained its disclosure is monitored and limited to authorized people for authorized purposes. And the final stage of good stewardship ensures that the personal information is deleted from all systems when the information is no longer needed (Straub and Collins, 1990).

In this study individuals expressed concern over the possibility of privacy breaches and the need to ensure their cloud service provider is protecting their information to the best of their ability. One participant stated,

“The cloud service provider should be financially responsible if any of my personal information is hacked.”

This statement effectively conveys the notion that the cloud service provider should have a certain level of fiduciary responsibility for protecting information that resides within their system. The intent of assigning a financial penalty or fine to the
failure of protecting information is to increase the awareness about the importance of good data stewardship. A privacy objective developed from this is to ensure that cloud service providers consider being data custodians as an important aspect of their service. These views place the sole responsibility of breaches on the cloud provider.

In contrast to this view, many of the participants believe in the notion that protecting privacy in the cloud is the responsibility of all parties involved. An individual stated the following,

“Due to the sensitive nature of personal information, I think the responsibility to protect the integrity and confidentiality of such information should not be only on the part of the cloud provider, rather it should be a shared responsibility between the owner of the information and the cloud services provider.”

Another participant stated the he believes that,

“There is a need for users to accept personal responsibility in the Cloud.”

A sub-objective derived from these statements is to ensure clearly defined responsibility structures for all parties involved towards information stewardship. In essence there is a shared belief that we need to increase individuals and cloud service providers’ awareness towards the responsibility of protecting personal information.

4.4.1.4 Maximize Individual’s Understanding of Cloud Service Functionality

The more an individual understands how technology works the less likely it is that they will erroneously disclose personal information that negatively impacts their privacy. Research suggests that individuals with a high cognitive understanding of technology will have a higher perceived self-efficacy with respect to using technology. This concept is supported by Social Cognitive Theory (SCT), which is widely used to
explain individual behavior (Bandura, 1986). Within Social Cognitive Theory literature, self-efficacy is considered to be an important influence on individuals’ behavior (Bandura, 1982). Self-efficacy is defined as a person’s judgment of his or her capabilities to perform a task. In the context of IT, the research suggests that individuals who possess high self-efficacy toward IT (otherwise known as Computer self-efficacy) are more comfortable using IT (Compeau, Higgins and Huff, 1999). Strecher et al. (1986) found that the effect of education or informative programs positively influence an individual’s self-efficacy and behaviors. Bandura et al. (1983) investigate the relation between self-efficacy and performance measures and found that they are positively related to each other. From this it is not to difficult to propose that an increase in individual’s understanding of cloud service technologies with respect to protecting privacy would lead to increased protection of individual’s privacy. Weisband and Reining (1995) finding that education or training experiences influence users’ privacy awareness support this argument.

During the interview process for this study several of the subjects requested for increased transparency from cloud service providers with respect to privacy policies and use of cloud technologies. One individual stated the following,

“I wish the cloud provider would provide more information to the user as to how information is handled or stored in the cloud.”

A second individual claimed that they believed,

“The more people know about how the cloud providers handle their information the more prepared they be will to act in a secure way.”

The general assessment from these comments is that cloud providers have
historically offered limited information about their technology infrastructure to their customers or consumers of their cloud products. One popular argument for not providing more transparency about IT infrastructures made by cloud providers is that it is a source of their competitive advantage. However as the concerns and issues surrounding privacy in the cloud become more prevalent cloud providers are going to have to be more transparent with their privacy practices in order to attract concerned users.

From a users perspective a better understanding of the cloud provider’s technology infrastructure allows them to be proactive in protecting their information on their end. One participant in the study claimed that,

“It is important to understand where the security architecture stops on the cloud providers’ side so that I can understand what I am responsible for and plan accordingly.”

Transparency about cloud provider’s privacy policies and practices allow for consumers to make informed decisions as whether or not to utilize the services of a cloud provider. One participant commented the following about his organizations adoption of the cloud,

“I wish management had understood our cloud providers privacy practices with respect to handling, storage and destruction of data before enlisting the services of the cloud provider.”

In other words the greater the understanding an individual or organization has about the services being provided by their cloud service provider the more prepared they will be to adequately protect their privacy and less likely they are to unknowingly disclose personal information.
4.4.1.5 Maximize Protection of Rights to Privacy

With recent privacy scandals such as news corps hacking of individual phone accounts of celebrities, politicians and even the general public as a means to gain access to personal information that is worthy to report in their tabloids, individuals are becoming increasingly concerned about information privacy and their right to it. Researchers in information systems literature have espoused the argument that with the increase of use of information within organizations today there is a need to protect both the individual and the organization in regards to information privacy issues (Freedman, 1982; Mason, 1986; Straub and Collins, 1990). Privacy has been defined as the right individuals have to control the collection and use of personal information about themselves (Mason, 1986). The right to privacy continues to be debated and is considered to be one of the most important ethical issues our time. While privacy has been declared a fundamental right by many international organizations such as the United Nations and the European Union, it is still being debated in the US as to what privacy rights exist within US legal system in regards to the protection of personal information.

During the interview process for this study the topic of “privacy rights” or “an individual’s right to privacy” came up several times. One participant stated that, “As an individual I should have the right to get documentation from any organization keeping data information related to me.”

The interviewee wants the right to know what information about him is being kept and how it is to be used. In the information privacy research literature, Freedman (1982) advocated a “right of information privacy” which proclaims that individuals have
the right to control the collection, storage, use, dissemination and accuracy of information stored about them.

Another individual who participated in this study shared their belief that,

“The right to privacy gives each person the right to have access to their personal information.”

This belief has been consistently supported in the information privacy literature. Mason (1986) supported the claim that individuals have the right to keep information about them private, assure that it is accurate, maintain ownership of it, and to have access to it. In order for individuals to be able to manage their privacy in the cloud they need to have the right to access the information being maintained about them such that they can take action to protect their privacy. Straub and Collins (1990) also discussed the protection of individual rights to privacy of information and suggested that individuals’ rights to privacy can best be protected through self-regulating policies and procedures. This argument supports the need for users to have access to adequate information about the cloud service providers privacy practices such that they can make informed decisions on protecting their privacy.

Another privacy issue identified in this study is a concern that organizations and cloud service providers will fail to meet their social obligations of protecting privacy. This concern was express by one individual in his statement that,

“I expect the cloud service providers to protect the rights of their customers.”

This statement seems to resonate with the notion of corporate responsibility where it is the responsibility of the “big” organizations to watch out for the “little guy.” Although not all organizations are good corporate citizens, but a good example of one is when IBM initiated its Four Principles of Privacy to protect privacy rights of employees.
(Carroll, 1991). Peter Drucker (1964) expressed that it is good business for corporations to be socially responsible. Along similar lines Straub and Collins (1990) argue that a main concern for all managers should be deciding how they collect and disseminate information on individuals while respecting individuals’ rights to privacy.

Another participant was concerned with understanding the boundaries surrounding the use of her personal information. She stated that,

“I wish I knew what rights the cloud service provider has with respect to using my information.”

Explicitly defining who has the legal right to individuals’ personal information is a bit challenging. An example which expresses this confusion about privacy rights is represented by the US Privacy Act of 1974 which protects individual privacy rights with respect to information held in government systems, however it does not apply to the private businesses. US Privacy laws do not protect privacy well and, in fact, are often behind the developmental trajectory of information technology (Henderson and Snyder, 1999). It has become best practice for organizations and individuals to enter into service agreements that specifically document information privacy practices.

The newness of the cloud environment has renewed individuals’ concerns about the uncertainty of legal protection for their rights to privacy. An individual stated,

“I want a contract where I can understand the legal aspects of the information once it is in the cloud’s possession, such as what rights they have use for, and what my rights to limit their use of my information.”

It is important for individuals and organizations to have well defined privacy agreements with their cloud service provider so that everyone knows who is responsible for protecting personal information and who has the right to access and use the personal
information being stored and maintain on the cloud resources.

4.4.1.6 Maintain the Integrity of Data

A primary goal of information integrity is to protect information from unauthorized modification (Joshi et al., 2001). Information integrity issues are commonly connected with improper storage of information where information is stored in a non-secure manner resulting in a lack of trustworthiness of the stored information, or lack of a proper authentication control for information access (Wang, Lee and Wang, 1998). This concern for proper storage controls for protecting data integrity resonated with a couple participants in this study. One individual stated,

“I am concerned that data integrity is at risk due to cloud vendor’s data storage techniques.”

Along similar lines another participant stated,

“I believe cloud providers need to ensure encryption mechanisms are utilized to ensure users that their information privacy and information integrity are safe.”

Both of these individuals expressed concern over the storage process in cloud computing. These concerns are rooted in the fact that the process of cloud computing relieves users and organizations from the burden of local data storage and maintenance. Therefore, these users and organizations no longer have physical possession of a large amount of their personal information and this makes ensuring data integrity in cloud computing a very important and formidable task.

Another primary risk to data integrity in cloud computing is the threat of commingling of data (Zhou et al., 2006). When data from one organization is combined or commingled with data another organization in the cloud, then it is much more vulnerable to being corrupted. A participant in the study proclaimed that they wished
“The cloud service provider would take adequate steps to ensure the integrity of my data.”

Wang et al. (2010) suggest that establishing an audit function for cloud data storage security is of critical importance so that users can resort to an external audit party to check the integrity of their data when needed. Antón, Earp and Reese (2003) noted the importance maintaining data integrity by ensuring data is both accurate and secure. They recommend organizations maintain the following integrity practices; providing consumer access to data; destroying untimely data or converting it to anonymous form; managerial measures to protect against loss and the unauthorized access, destruction, use, or disclosure of the data; and technical measures to protect against loss and the unauthorized access, destruction, use, or disclosure of the data. We believe cloud service providers should adopt these integrity practices as well.

4.4.2 Means Objectives for Ensuring Cloud Privacy

4.4.2.1 Maximize Effectiveness of Secure Data Transfers

Secure data transfers should be a concern for all of the traffic travelling between private networks and whatever cloud service is being used because all of the data must at some point in time traverse the Internet. Our participants expressed this concern as well, one individual stated,

“I believe cloud providers should develop standards for the data format for data transfers.”

Researchers have recommended that data in transit should be encrypted and authenticated using industry standard protocols, such as IPsec or SSL that have been developed specifically for protecting Internet traffic (Agudo et al., 2009). This is because the simplest way to increase privacy protection is to encrypt its data before sending it to the cloud.
Similar concerns for secure data transfers were expressed by other participants. One participant stated they believe that

“Data should be encrypted when it is transferred between vendors.”

While another stated,

“I wish that my data would not be corrupted during data transfers.”

A challenge to securing data transfers via encryption methods prior to sending it through the cloud is that the level of complexity is increased which result in lower efficiency of the data transfer process. As a solution to this efficiency problem, researchers suggest classifying data, based on significance and sensitivity, into well defined privacy categories before uploading data to be stored and processed in the cloud (Itan, Kayssi and Chehab, 2009). It is important that cloud service providers understand the importance of clearly establishing well-defined secure data transferring practices.

4.4.2.2 Optimize Ease of Use of Cloud Technology

The concept of ease of use or perceived ease of use as it relates to technology has been extensively research over the past decades (Rogers, 1962, Hernandez and Mazzon, 2007; Eriksson, 2005; Venkatesh and Davis, 1996; Venkatesh and Morris, 2000). Rogers (1962) noted that the understanding technology, which leads to the adaptation of innovative service/product by customers, is known as ease of use. Perceived ease of use has been defined as the degree to which a person believes that using a particular system of type of technology would be free of effort (Davis, 1989). While ease of use may be good for technology adoption careful consideration need to be given the design of cloud computing applications to ensure that it is supporting strong privacy controls and not weakening the privacy environment.
Research has shown that there is a natural dichotomy between the concepts of “ease of use” and “privacy”. Feigenbaum et al. (2002) identified a critical concern with privacy-enhancing technology to be the apparent tradeoff between ease-of-use and security. Many ease-of-use issues are related to the problem of authentication. While it is important to ensure ease of access for authorized users to gain access to the information it also important to ensure proper controls are in place to ensure the authentication process is secure. One aspect of how ease of use can be used to enhance privacy controls was suggested by one of our participants who stated.

“I wish that I could remove obsolete data with efficiency and ease.”

In order to facilitate stronger privacy controls the ease of use technology it best to develop privacy-enhancing tools, which can be easily adopted by cloud users.

4.4.2.3 Maximize Technology Infrastructure Competencies

With the rapid expansion of cloud computing researchers have noticed that maintaining the levels of protection of data and privacy required by legislation in cloud computing infrastructures is a major challenge (Pearson and Charlesworth, 2009; Dhillon and Kolkowska, 2011). The nature of open networks such “the cloud” is that they are accessed via the Internet, which contain several access points that are potential targets for hackers to penetrate an organization. This concern towards being hacked was voiced by several participants who stated they believe

“There is an increase risk of hacking of cloud computing resources”.

Through probing discussions questions on this topic they stated that because of the increase concentration of data being stored in the cloud they believe that hackers will start to target cloud servers more because of the possibility of gaining access to a lot
more information they if they went after a single provider’s servers. This fear of being hacked also had them concerned that the encryption technology being used in the cloud is not adequate for the cloud environment. These concerns led to the development of the following privacy sub-objective: To ensure technical security measures are being used to protect my personal information.

Pearson and Charlesworth (2009) proposed that procedural and technical solutions be co-designed to demonstrate accountability as a means to resolve privacy issues within the cloud. Researchers have argued that IT practitioners need to focus on technical measures necessary to provide a secure IT environment that effectively protects consumer privacy (Earp, Anton and Jarvin, 2002). It is well acknowledged by researchers that tools and technical controls alone cannot fully address privacy issues in cloud computing (Dhillon and Kolkowska, 2011). However, privacy in the cloud would be impossible without proper IT technical controls in place (Pearson and Charlesworth, 2009). It is best that privacy protecting controls be build into all aspects of business processes whether they are technical or social-technical.

4.4.2.4 Minimize Unnecessary Access to Information

Smith et al. (1996) identified improper access as being a major concern for privacy. In the context of personal information privacy it is concerned that a user’s personal information is protected from unauthorized access and use (Skinner, Han and Chang, 2006). Madden et al. (2007) found that 85 percent of adults surveyed believed it was “very important” to control access to their personal information. Who should be allowed to access personal information has been an on going debate within the privacy literature. This is a question not only of technological constraints but also of
organizational policy (Smith et al., 1996). A majority of the participants were concerned with unauthorized access to their information. One participant stated,

“I would like to know who has access to my information and believe that it is a cloud providers responsibility to clearly communicate it to me”

Another participant to stated the following

“I like it when I have the ability to set controls as to who can view my information”

Pearson and Charelesworth (2009) identified several ways in which inappropriate or unauthorized access to personal data in the cloud is granted such as lack of access control enforcement, policies being changeable by unauthorized entities, or uncontrolled and/or unprotected copies of data being spread within the cloud. Stringent access controls to prevent unauthorized access to the data must be provided by cloud service providers (Kaufman, 2009). Leavitt (2009) suggest that cloud service providers should not pass audits of their capabilities by prospective clients if they can’t demonstrate who has access to their data and how they keep unauthorized personnel from retrieving information. We believe that limiting unauthorized access to personal information is essential to ensuring privacy in the cloud.

4.4.2.5 Increase Standardization of Cloud Technologies

The rapid development of the cloud-computing environment has resulted in a lack of industry standards for delivering and monitoring of cloud services. Having cloud standards would help with technical aspects of cloud computing like interoperability and virtualization. Interoperability between one cloud provider and another is very important because it allows for information from one application to seamlessly interact with another application which would help customers to maximize efficiency and
thus their return on their technology investments (Ortiz, 2011). Virtualization’s flexibility lets cloud providers to optimize workloads among their hardware resources. While having standards would help with these technical concerns of cloud computing it is also very important for ensuring privacy in the cloud as well. Researchers have expressed the need of having standards for cloud computing. Marston et al. (2011) posit that cloud computing raises new privacy issues that require clear standards for custodians of this information. They argue that cloud computing needs a set of regulations that explicitly define the responsibilities of an organization with respect to its cloud data. However, they also point out that such regulation will also need to be cognizant of existing privacy laws. This in itself can be challenging due to the fact that there are significant differences between the E.U. and the U.S. approach to privacy protection (Kauffman et al. 2011). Individuals from our study expressed concern about the development and monitoring of cloud standards along various perspectives. One individual claimed that,

“Cloud providers should develop standards for the data format for data transfers.”

And another stated,

“That regulations and standards are important for establishing a cloud structure that supports data privacy.”

While the creation of cloud standards will go along way to establishing a minimal level of privacy expectations for cloud computing customers it will still have to evolve and adapt to future changes in cloud computing technology. According to Pearson and
Charlesworth (2009) cloud service providers will have to review and improve their privacy standards on an ongoing basis. Aguliar (2000) proposed an approach to online privacy protection, and called for government-enforced self-regulation that can be adopted by the cloud computing industry as well. In this approach, there is a partnership between industry and government with respect to creating and governance of standards and regulations. One way this approach could be designed is to have industry leaders participation in creating regulations where industry standards become enforceable by law or other self-regulatory enforcement processes that come to be government sanctioned (Kauffman, Lee, Prosch and Steinbart, 2011).

**4.4.2.6 Optimize Effectiveness of Privacy Policy Governance**

It is important that cloud users are informed about their cloud service provider’s privacy policies so they can effectively govern their privacy exposure. Gartner Group recently reported that 50% of all enterprises will revise their corporate privacy policy requirements in order to reflect changes in business practices, such as the use of cloud computing and location-based services available on smartphone. From a user’s perspective privacy risks vary significantly depending on privacy policies established by the cloud provider (Subashini and Kavitha, 2010). Pearson and Benameur (2010) discuss how privacy risk in cloud computing can be reduced if organizations involved in cloud provision use a combination of privacy policies and contractual terms to create accountability. One reason individuals or companies are exposed to privacy threats is because they either did not read or understand their provider’s privacy policy statement. According to Cranor (2003) consumers find privacy policies time consuming to read and difficult to understand, and readability experts have found that
comprehending privacy policies typically requires college-level reading skills. In addition she found that consumers who do read these policies are also frustrated by the fact that they can change unexpectedly. A participants in this study have expressed concern that

“my cloud service provider my data and their privacy policies are not transparent enough for me”

Another participant shared similar concerns in that,

“I have an issue with companies that changes their privacy policy agreements after I have already signed up for their service, I know it is important to stay current with the required regulations but I still like to be at least notified of the changes before hand”

Having a good privacy policy that defines what data is collected, for what purpose the data will be used, whether the enterprise provides access to the data, who are the data recipients, how long the data will be retained, and who will be informed in what cases is a privacy practice (Karjoth and Schunter, 2002). It is important that privacy policies are clearly and explicitly stated because it will increase the customer’s perception that the organization can be trusted (Earp, Antón, Aiman-Smith, and Stufflebeam, 2005). Thus, it can be important to the bottom line of an organization to alien their privacy policies and policy statements with their customers’ privacy values.

4.4.2.7 Maximize Performance of Privacy Risk Assessments

Organizations, businesses and individuals considering cloud-based services must understand the associated privacy risks associated with it and take those risks into consideration when deciding whether or not to use it (Svantesson and Clarke 2010). The Gartner Group reported that the cloud has unique attributes that require risk assessments for areas such as privacy and security (Brodkin, 2008). Risk assessments allow
organizations to evaluate their privacy, security, and compliance controls as a means to protect against future losses (Kaliski and Pauley, 2010). The process of performing a risk assessment includes the following five steps: identify system characteristics, threat assessment, vulnerability analysis, impact analysis, and risk determination (Chen, 2009). Once a risk has been identified it is important to define acceptable use cases and necessary compensating controls before implementing a cloud based solution. Several participants in this study shared this belief for instance one individual expressed that

“It is important to understand all the risks prior to using the cloud.”

Another stated that

“I am concerned with the level of risk associated with storing data in the cloud because I have less control over my data.”

It is important to ensure that not only that risk assessments are performed adequately but also that when possible the results of the assessments are shared or communicated with the users of the cloud services. Flavián and Guinalíu (2006) claimed that clearly communicating privacy statements, security policies and assessments are effective methods for establishing trust in online service providers. Cloud service providers are beginning to adopt the practice of performing risk assessments as a means to relieve customers concerns about their privacy practices. A resent example of this is Amazon Web Services (AWS)’s news release that it had passed a SAS 70 Type II Audit. This notion of effectively communicating assessment results is also adopted by the federal government in the E-Government Act of 2002. The E-Government Act requires all federal agencies to have a Privacy Impact Assessment (PIA) completed for all new or substantially changed technology that collects, maintains, or disseminates
personal identifying information and to make the results publicly available. A PIA is a structured review of an information system to identify and mitigate privacy risks at every stage of the system lifecycle (Jansen and Grance, 2011). The E-Government Act was intended to assess privacy issue dealing with web based government applications and is applicable to cloud-computing services. Cloud computing technologies should not be used unless the user can ensure that privacy risks are satisfactorily addressed and privacy laws are complied with.

4.4.2.8 Increase Control Over Information Disclosure

Zissis and Lekkas (2012) claim privacy is the desire of a person to control the disclosure of personal information. This concern for control over personal information disclosure has been well documented and linked to individual’s concern for privacy in IS literature. Westin (1967) focused on information disclosure and defined privacy as an individual’s claim to be able to self-select when, how and to what extent their information is communicated to others. Margulis (2003) developed a behavioral perspective of privacy where he identified two important factors of privacy: control over disclosure of personal information and a notion of vulnerability. Recently, the world privacy forum developed a list of privacy issues for cloud computing, most of which are concerned with the disclosure, jurisdiction, and legal aspects of information privacy (Gellman, 2009). An individual stated the following with respect to their concern for responsible disclosure of privacy breaches,

“Before committing to a cloud service I wish I knew the history regarding how many times it has been hacked successfully and the number of times their system has crashed and for how long
The threat of disclosure of sensitive private information when exchanging data through a cloud service needs to be assessed. By evaluating this risk the exposure of personally identifiable information should be limited (Wang, Zhao, Jiang, Li, 2009). As a means to protect user’s privacy in cloud computing Pearson and Charlesworth (2009) argued that users must be given the choice of whether they want their information to be collected or not. In essence data subjects should be requested to give their consent to the collection, use and disclosure of their personal identifiable information. In order to maintain trust relationships with their users it is important that cloud service providers uphold the their end of the privacy agreement. Therefore, data should only be used or disclosed for the purpose for which it was collected and should only be divulged to those parties authorized to receive it. Personal data should be aggregated wherever possible to limit the potential for compute matching of records. Personal information should only be kept as long as is necessary. By requesting users consent to data collection and usage practices the cloud service provider can help increase users control over information disclosure and thus help ensure their privacy in cloud computing.

4.4.2.9 Ensure CSP has Effective HR Practices

Organizations have the responsibility to establish effective controls to ensure that privacy policies and procedures are being followed. Having good human resource (HR) practices is a necessity to ensure the protection of individual’s personal information. HR practices should be designed to protect both the internal and external customers. It is in the best interest of the cloud service provider to have HR practices that support the
privacy policy and practices they have established. One of the biggest threats to any organization’s privacy and security policies is an internal threat of an employee error or intentional act. An individual in our study expressed this concern about the ethical behavior of internal employees when he stated that,

“I wish the cloud provider performed a through background check before hiring new employees.”

An important control against these internal threats is to ensure that all company employees have been trained properly about privacy controls and technology usage. Employee training is a good way to increase awareness about privacy risks however it will not prevent intentional act of employees to steal customers personal information or to cause harm to the company. Therefore, it is important for companies, including cloud service providers, to verify previous work experience and to conduct background investigations of new employee candidates. This will reduce the likelihood of hiring an individual of questionable character who could potentially be a risk to the company and customers’ privacy expectations.

4.4.2.10 Minimize Government Access to Information

Recent government actions towards the confiscation or seizure of cloud servers has heighten individuals concern about “big brother” monitoring their computing activities. People do not like the notion that there is a possibility that their actions are being monitored, tracked and possibly shared without their consent. Historically when the government decides they need access to data stored on a server they simply take control of the server, bank of servers or even all the servers owned by a cloud storage provider as they did in the case of Megaupload. This type of action on behalf of the government is a disruption to all parties who have personal or business
related data stored on the seized servers. It appears that individuals’ concern about
government seizure of cloud storage servers is less about protecting their illegal activity
and more about ensuring they have access to their files and information. Individuals
have mixed feeling with regards to government role in monitoring and governing cloud
computing activities. On one side individuals want the government to establish
regulations to protect their information privacy rights and on the hand they do not want
the government to monitor individual activities because they feel their privacy is being
infringed upon. An individual concerned with the protection of their privacy rights stated
made the following claim,

   “I am concern that US laws give government power to access my private information.”

   Another participant expressed the following concern,

   “I believe American laws such as the US Patriot Act provide the government with virtually
   limitless powers to access information including that belonging to companies.”

   Nissenbaum (2004) considered limiting surveillance of citizens and use of
information about them by agents of government an important guiding principle in the
protection of the contextual integrity of privacy. According to this principle privacy is
protected by well defined, and generally accepted political principles addressing the
balance of power, which, among other things, set limits on government intrusiveness
into the lives and liberty of individuals (Nissenbaum, 2004) It is important to the
longevity of cloud computing and individuals’ privacy rights to limit the action of the
government with regards to unjustified or unwarranted data gathering or surveillance of
general citizens.
4.4.2.11 Maximize Effectiveness of Independent Oversight of Privacy Practices

Independent oversight of privacy practices refers to a third party verifying that an organization, such as a cloud service provider, is adhering to their stated policies and regulatory requirements. When individuals or organizations decide to use a cloud service the decision process is similar to other web-based transactions in that there needs to a certain level of trust between all parties involved. One way to establish and build trusting relationships between organizations and their stakeholders is by having an independent audit performed of the organization’s policies and practices and their ability to meet regulatory requirements. Moores and Dhillon (2003) noted that the e-commerce industry utilized privacy seals to install trust by verifying that the web site has a policy about its collection and use of personal identifiable information. While privacy seals were initially created to build trust relationships between consumers and e-commerce websites they are being used in cloud computing environments as well. Recently TRUSTe a leading online privacy seal and services provider created TRUSTed Cloud Data Privacy Certification program to help cloud providers build trust with future consumers. Privacy seals provide some level of comfort to consumers such as verifying that stated Privacy policies are being followed. However they lack substance in comparison to a SAS 70 audit or other detailed privacy audits performed by a reputable third party. Several of the interviewees in this study expressed concern towards having the ability to requests an audit of their cloud service provider. One participant stated the following with respect to this concern,
“I wish proper access controls such as authentication and authorization and auditing of these controls are well established by the cloud provider.”

The importance of having effective independent oversight of privacy practices is paramount to ensuring privacy in cloud computing. Wang et al. (2010) suggest that performing an audit of cloud data storage providers is important to ensuring data integrity and privacy in cloud computing. Probst et al. (2012) even go as far as to recommend the creation of a public penetration-testing agency as a means of increasing customer’s trust in cloud providers.

4.4.2.12 Optimize Access Controls

The control of access to personal information has been espoused to be a critical component of privacy. Smith (1993) identified unauthorized access to information a primary concern for information privacy. Individuals concerned with protecting their privacy regulate social interactions by selectively controlling access to one’s self (Altman, 1977). Within the realm of technology usage this means individuals need to protect and control access to their personal information stored on databases or servers that have come in contact with. This process may seem a bit daunting when dealing with the vastness of cloud computing environment. It is essential to the protection of users’ privacy that stringent access controls to prevent unauthorized access to personal data are provided by cloud service providers (Kauffman, 2009). Several of our participants expressed the concerns about the need of maintaining strong access controls such as the following statements,

“I am concerned about password protection and identity theft if my information gets into the wrong hands.”

“I believe it is important to determine who should have access to what for ensuring the privacy rights.”
Optimization of authentication tools, access controls and audit practices helps to build a foundation for protecting personal information (Sandhu & Samarti, 1996). Authentication is the process of establishing the identity of one party to another. To ensure access is only granted to those who are authorized to have access it is important to ensure that the individual or system being granted access as been verified to be who they say they are. The typical authentication process is based on either something the user knows, something the user possesses, or something the user is (Sandhu & Samarti, 1996). Something a user knows usually refers to a password. Something a user possesses can be a cryptographic token or smart card. Some the user is can be captured through biometric signatures such as fingerprints, eye scans, or voice recognition. The best authentication process requires a combination of any two of these of these authentication methods. Sandhu & Samarti (1996) explain that once authentication has been verified having well defined access controls determines what one party will allow another to do with respect to resources and objects mediated by the former. Common methods for controlling access are as follows:

- **Discretionary access control (DAC)** requires that the owner of data should determine who has access to it (Sandhu and Samarati 1994).
- **Lattice-based access control** more commonly refer to mandatory access controls (MAC), restricts the transfer of information to one direction in a lattice of security labels such as low to high but not high to low (Sandhu 1993).
- **Role-based access control (RBAC)** requires that access rights be assigned to roles rather than to individual users thereby requiring users be assigned to the appropriate roles in order to obtain certain access rights (Sandhu et al. 1996).

Once authentication process and access controls have been defined Sandhu & Samarti (1996) argue that performing an audit of these practices is next necessary step for ensuring protection of personal information. An effective audit process
gathers data about activity in the system and analyzes it to determine if there are any security or privacy violations (Lunt 1993; Mukherjee et al. 1994).

4.4.2.13 Optimize Segregation of Information

The notion of maintaining the integrity of data by clearly defining processes to separate data is not new in the field of information systems or privacy research community. Smith (1993) identified information errors to be a primary concern for information privacy. This acknowledgement led to researchers and practitioners developing practices to clearly separate data held within databases as a means to reduce informational errors and protect information privacy. The importance of data segregation has re-emerged as a hot topic with the recent advancements in cloud computing. Cloud Security Alliance and Gartner Group identified shared technology and data segregation as a top ten security and privacy concern of cloud computing. Ensuring proper controls surrounding personal data segregation also emerged in our discussions with our study’s participants. For example a participant stated that,

“It is important to segregate information about myself into specific identity groupings such as personal, family, friends, professional, academic.”

Another expressed the following

“I expect my personal information to be compartmentalized within the server based on who needs to view the information.”

Cloud infrastructures are typically designed to support a concept of multi-tenancy where multiple users can store their data in the same location. There is a resulting challenge with public cloud infrastructures because they are not designed for compartmentalization and are thus prone to certain vulnerabilities that can be exploited.
One such risk is that of data exposure of one user’s data to another in this type of environment. Clear boundaries for each user’s data must be established at both the physical and application levels (Subashini & Kavitha, 2010).

**4.4.14 Minimize Third Party Access to Information**

Limiting third party access to personal information is at the very core of the definition for personal information privacy. Personal information privacy has been defined as the ability of the individual to personally control information about oneself (Stone, Gardner, Gueutal, and McClure, 1983; Milburg, Burke, and Smith, 1995). Individuals in this study has expressed the desire to ensure that personal information is not collected, used or disseminated to unauthorized third parties. For one individual stated that

“I wish my cloud service provider would notify me and give me the choice to disclose my information to a third party or not.”

There is a significant challenge to limiting third party access in cloud computing environments. A popular business model for cloud service providers is to provide a cloud service to users for free so that can establish traffic to their site so they can generate revenue from third parties (Dhillon and Kolkowska, 2011). Therefore it is important for cloud users to verify data sharing practices of the cloud provider they are planning to use. Another precaution users can take is to request periodic audits of who has been granted accessed their data files.

**4.4.2.15 Minimize Liability Concerns**

Cloud users need to cognizant of legal risks associated with its usage. For example a key feature of public clouds is the pooling of resources using
shared infrastructure to collect, process and store data. The concern here is that it is near impossible to determine where the data resides in the system at any given point in time. This uncertainty with regards to the location of stored data results in possible legal issues due to jurisdictional privacy requirements (Sotto et al., 2010). For example if personal data is stored in a country other than its owner, there is uncertainty as to which country’s privacy laws must be followed to be compliant. Given the complexity of regulatory issues across various jurisdictions the inability to know where one’s data is located is a legal liability to organizations using cloud services. This uncertainty with respect to legal obligations was a significant concern amongst our study’s participants.

An example of an individual expressed the following,

“I am concerned that if the cloud provider does not protect the data as required by my local laws I may be held responsible.”

Using a cloud service provider can potentially result in numerous state and federal privacy requirements. In the U.S. certain regulatory frameworks require data owners to ensure third party service providers are capable of maintaining the privacy of personal information entrusted to them. Two specific regulatory frameworks that are relevant with the storage of personal information in the cloud are Health Insurance Portability and Accountability Act of 1996 and the Gramm-Leach-Bliley Act. These two acts are designed to protect select types of sensitive personal information (i.e. personal health information and personal financial information. However, there are similarities between them. For example both acts require organizations to enter into a contract with their service provider that prohibits the service provider from disclosing or using the information other than to carry out the purposes for which the information was disclosed.
(Sotto et al., 2010). The legal concern of using the cloud is not limited to only U.S. companies; they also are relevant to companies operating or providing services in Europe. For example under EU data protection laws, organizations that “process” personal data must have a legal basis for doing so: and uploading data into the cloud is considered “processing” in the European Union. Given that the legal landscape as it applies to privacy regulations is a complex matter and is constantly changing it is important for cloud users to continuously review their own jurisdiction’s privacy regulations as well as international privacy laws.

4.4.2.16 Ensure Cloud Service Provider has Effective Internal Controls

Maintaining protection of data and privacy required by current legislation in cloud computing is challenging. Pearson and Charlesworth (2009) states that creating accountability towards privacy in an organization is important to ensuring privacy in cloud computing. This can be achieved by designing privacy-protecting controls into various aspects of the business process. Jensen and Grance (2001) argue that secure privacy practices entail monitoring an organization’s information system assets and assessing the implementation of policies, standards, procedures, controls, and guidelines that are used to protect information privacy. Assessing and managing privacy risk in the cloud can be a bit of a challenge, since significant portions of the computing environment are under the control of the cloud provider and may likely be beyond the organization’s purview (Chow et al., 2009). A lack of transparency on behalf of the cloud provider in regards to their privacy practices is a concern to many individuals. An individual expressed the following concern,
“I wish I knew what controls are in place to protect my information in the cloud.”

Another participant concerned with cloud controls stated that,

“I wish proper access controls such as authentication and authorization along with a requirement for auditing of these controls are well established by the cloud provider.”

Strong management practices are essential for operating and maintaining a secure cloud computing solution. Dhillon (2001) argued that successful implementation of internal controls is key for running a ‘well-oiled’ business. COSO’s Internal Control-Integrated Framework defines internal control as a process designed to provide reasonable assurance regarding the achievement of objectives in the following categories: a) Effectiveness and efficiency of operations; b) Reliability of financial reporting; and c) Compliance with laws and regulations. Typically internal controls designed to protect information privacy are usually concerned the latter of these, compliance with laws and regulations. COSO defines internal control as having the following five components:

- Control Environment-sets the tone for the organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control.
- Risk Assessment-the identification and analysis of relevant risks to the achievement of objectives, forming a basis for how the risks should be managed.
- Information and Communication-systems or processes that support the identification, capture, and exchange of information in a form and time frame that enable people to carry out their responsibilities.
- Control Activities-the policies and procedures that help ensure management directives are carried out.
- Monitoring-processes used to assess the quality of internal control performance.
over time.

Management needs to consider these five items in order to design and implement an ideal set of internal that provide assurance that the organization’s control objectives are being met (Dhillon, 2001). For a cloud provider it is important that can effectively implement privacy controls necessary to protect the user’s personal data and provide evidence about the effectiveness of those controls. It is important to realize that the effectiveness of internal controls depend on the competency and dependability of the people using it (Dhillon, 2001). Therefore it is important to monitor these controls through a privacy audit function to ensure information privacy is being maintained in the cloud. Pearson & Charlesworth (2009) claim that it is the responsibility of an organization to conduct privacy reviews throughout the life of the contract with the cloud service provider. Continuous monitoring of information privacy requires maintaining ongoing awareness of privacy and security controls, vulnerabilities, and threats to support privacy risk management decisions.

4.4.2.17 Maximize Availability of Cloud Resources

Based on the investigation to those Cloud Computing systems, we find that the security and privacy concerns provided by companies nowadays are not adequate, and consequently result in a big obstacle for users to adapt into the Cloud Computing systems. Hence, more concerns on security issues, such as availability, confidentiality, data integrity control, audit and so on, (Zhou et al, 2010). Having the ability to control access to one’s personal information is and important aspect of information privacy. Reducing the likelihood of unwarranted access requires stringent access
controls to prevent unauthorized access to personal data (Kauffman, 2009). However, if the system denies the owner of the information access to their own information when they desire access, it will impact the cloud users perception about the controls or lack of proper controls of the cloud service provider. A participant in this study expressed the following concerns with regards to the availability.

“I am concerned about the reliability of access to my data.”

The primary concern with the lost of availability to access ones information stored in the cloud is that the user starts to lose trust in the cloud service provides ability to maintain control of their systems. Therefore if the cloud service provide cannot assure access to my information how can they adequately protect my information or privacy. Managing trust perceptions such as these is an important aspect of managing consumer privacy concerns (Campbell, 1999; Gengler and Leszczyc 1997). While it is impossible to guarantee 100% availability cloud service providers need to maintain high levels of availability of their cloud servers to meet customers’ expectations and maintain their trust in the cloud system.

4.4.2.18 Increase Awareness of Data Ownership

The distributed nature of cloud computing is changing the notion about data residency and data ownership (Marston et al., 2011). The question of who owns the data in the cloud is an important question, some argue that the data is owned by the company who is collecting the data, some say that the data is owned by the cloud service provider where the data is being stored, while others claim the data is owned by the individual the information is about. It is essential that this question of data ownership be resolved
before an organization adopts a cloud computing strategy (Katzan, 2010). Consumers and businesses used to not only own their data, but also controlled how that data was to be used, now companies in the process of converting to cloud computing are simply handing over their data to a third-party service providers, who store the data in the cloud with limited knowledge as to who has ownership rights of the personal data (Marston et al. 2011). There are numerous privacy and legal issues that are associated with the responsibility of data ownership that need to be considered when implementing a cloud strategy. With respect to this concern an individual expressed the following

“I believe users should have more control and the right to own their own data even when using services of a cloud provider.”

A participant stated the following

“I believe people should be responsible for their own data.”

Recognizing individual’s rights to data ownership is an important step in establishing trust in online environments (Hoffman et al., 1997). Ensuring privacy in a cloud-computing environment is requires a level of trust between individuals and their cloud service provider. Trust can be encouraged by cloud service providers by allowing the balance of power to shift towards a more cooperative interaction process with their customers (Hoffman and Novak, 1997). Part of this cooperative process should include an opt-in or opt-out option with respect to personal information being collected by the cloud provider. Jansen and Grance (2011) argue that an organization’s data ownership rights need to be firmly documented in a service agreement contract to enable a basis for trust and privacy of data. Typically service agreements are non-negotiable in most public cloud computing environments, however negotiated service agreements are
possible. A well negotiated agreement on behalf of an organization or individual will clearly state that they retain exclusive ownership over all their data; and that the cloud provider has no rights or licenses through the agreement to use the data for its own purposes (McDonald, 2010).

4.4.2.19 Ensure Service Level Agreement Meets Privacy Requirements

The specifications of cloud services and service arrangements between the cloud service provider and the cloud user in a form of a service contract or service agreement. These service agreements typically outline the terms and conditions regarding access and use of the cloud services being offered. It also will include contractual aspects of the agreement such as the period of service, conditions for termination, and destruction of data procedures upon termination. These terms and conditions are usually documented in multiple documents such as service level agreement, privacy policy, acceptable use policy, and terms of use policy (Bradshaw et al., 2010). The service level agreement communicates the understanding between the cloud user and the cloud providers about the level of service that can be expected, and what the compensation would be to the user if the provider fails to deliver the cloud service at the level specified. These service level agreements can also be drafted to include compensation or ensure mitigating controls are activated if the cloud providers fail to meet privacy agreements or regulations. Some of the participants in this study were concerned about their cloud service provider’s service contracts and their comment to ensure that their stated privacy policies are adhered to. One individual commented that,
“it is important to have a well-documented contract with the cloud service provider to ensure access to my data in the case the service provider goes out of business.”

Another individual participating in the study claimed that.

“It is important to me that the cloud provider does not change his terms of service”

Bradshaw et al. (2010) found that while cloud computing is an attractive option to users who are experience rapid growth or are unsure of the what their computing infrastructure requirements will be like in the future due to variable and unpredictable technology demands. However in their analysis of cloud providers’ service contracts, they noted that this great level of flexibility offered by Cloud computing is offset by less certainty for the customer in terms of the location of data and the legal foundations of any contract with the provider. Jansen and Grance (2011) argue that it is best to negotiate a service agreement with a cloud provider instead of accepting their standard agreement. Items such as the vetting of employees, data ownership and exit rights, breach notification, isolation of tenant applications, data encryption and segregation, tracking and reporting service effectiveness, compliance with laws and regulations, and the use of validated products meeting federal or national standards can be include in the negotiated service agreement.

4.5 Evaluation of cloud privacy objectives

It is important to evaluate fundamental and means objectives we have identified in this study to ensure their validity. As described in chapter 3 we utilized experts to validate the objectives for ensuring privacy as recommended by Dhillon and
Torkzadeh (2006). An audit team that consisted of 6 individuals with an expertise in auditing information systems performed the evaluation process. These experts were utilized to evaluate the validity of the objectives for ensuring privacy in cloud computing. They reviewed the 23 identified main objectives for ensuring privacy in cloud computing identified during the data analysis of VFT phase of this study. Each member of the audit team reviewed the 23 main objectives and the clusters of sub-objectives individually to determine if they considered them to be valid objectives for ensuring privacy in cloud computing. During this process they also evaluated the relationship between each main objective and its corresponding sub-objectives and determined if they were accurately group together in their professional opinion. Once each member had reviewed the objectives we had a focus group meeting and they shared their opinions on the validity of the objectives. After this discussion, the group decided one objective, “To maximize availability of cloud resources,” initially classified as a fundamental objective should be classified as a means objectives. Also, the group determined that the following two additional objectives needed to be include in the list of means objectives, “Increase awareness of data ownership” and “To ensure service contract meets privacy requirements.” This resulted in a total of 25 main objectives being identified, 6 fundamental objectives (see table 4.1) and 19 means objectives (see table 4.2). These 25 cloud privacy objectives will be discussed in the detail below in the results section.

4.6 Discussion on the cloud privacy objectives

Threats to privacy are an increasing concern for business leaders today. This is because privacy issues are a concern to all types of stakeholders. These issues
are also compounded in cloud computing environments due to the pervasive nature of how personal information is collected and process and used within the scope of normal business activities. Privacy threats to an organization using a cloud service, such as data leakage, information disclosure issues, failure to comply with required regulations expose that organization to risk of legal liability or credibility concerns if or when a privacy breach occurs. It is in the best interest of a company towards its longevity to proactively manage threats to privacy than to simply respond to a privacy breach after it has already occurred. This means that it is important for organizations to develop privacy management practices that are socially responsible towards the protection of privacy.

Managing privacy in the cloud is a challenge because the complexity that is involved with managing the collection, storage, processing and use of information across multiple technology platforms and jurisdictional boundaries. This level of complexity requires that management be well informed as to the privacy expectations of all their stakeholders before they develop their corporate strategy towards the use of personal information throughout their organization. Understanding the privacy objectives identified in this research will provide insight to management as to what privacy controls need to be established protect privacy in the cloud. Strong privacy controls are require to in order to instill public trust in a company’s their ability to protect privacy. An understanding of these privacy objectives will assist management in making key decisions as to how effectively manage privacy in the cloud.

Building consumer trust is an important goal for any company. We found that
individuals are wary of the potential for lack of controls or ethical standards on behalf of the cloud provider. Trust is an important item in the process of ensuring the protection of information privacy. Trust has been defined as "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party" (Mayer, Davis, and Schoorman, 1995; p. 712). Trust in the cloud is the degree to which the cloud user can rely on the assertions or information provided on the behalf of the cloud service. Privacy managers can increase institution-based trust mechanisms by developing privacy practices that support the cloud privacy objectives. Institution-based trust is the belief that the required structural conditions for achieving a successful outcome, such as the protection of information privacy, are present (McKnight, Choudhury, and Kacmar, 2002). Within the increase trust with the cloud provider objective there are several guidelines that help management to build institution-based trust measures. Maximizing effectiveness of secure data transfers, which helps to build trust in the information technology infrastructure, or maximizing the performance of risk assessments helps to ensure organizations are evaluating their systems to ensure risks are reduced. By establishing trust in their cloud privacy practices a company can build customer loyalty. This increase in trust and customer loyalty provides an opportunity for management of company to lower its transactional costs and increase profitability.

Adhering to the cloud privacy objectives identified in our study also assist management in developing an effective set of internal controls for protecting privacy and ensuring proper governance of cloud privacy practices. One key aspect
of a good internal control system is the establishment of accountability of stakeholders operating within the system. Pearson and Charlesworth (2009) argued that there is a need to increase accountability in the cloud provider as a means for protecting privacy in the cloud. The cloud privacy objectives encourage the notion of accountability through several of the identified objectives. For instance, accountability is supported within the cloud privacy objective of increasing information stewardship. The concept of information stewardship conveys a fiduciary level of responsibility toward data management practices for the cloud service provider (Rosenbaum, 2010). This implies that there is a risk of a financial penalty if the cloud service provider fails to protect a user's information privacy.

Protecting the company from legal liabilities and unnecessary financial risks is an important aspect of management responsibility. Having a good understanding of the cloud privacy objectives helps management to facilitate the protection of information privacy by encouraging cloud service providers and users to evaluate the legal requirements for protecting information privacy before providing or utilizing a cloud service. It is important for individuals and organizations to have well-defined and legally binding privacy agreements with their cloud service provider so that everyone knows who is responsible for protecting personal information and who has the right to access and use the personal information.

Another means to reduce legal and financial liability is through strong independent oversight of privacy practices. By having an independent audit or review performed on a regular basis it ensures that the cloud service provider is adhering to
their stated privacy policies and practices. It also helps to ensure that the cloud provider is incorporating any new privacy requirements into the privacy policy and practices. The cloud privacy objectives establish a good foundation from which a cloud privacy audit could be designed. An effective cloud privacy audit program ensures stakeholders that operational practices with respect to information handling practices in the cloud are effective and meet regulatory standards. An Audit also provides management with additional information to develop or acquire necessary tools or resources to improve their information handling practices, such as, creating a cloud privacy strategy, evaluating cloud privacy practices, and improving the audit process itself.

Conclusion

This chapter presented the fundamental and means objectives for ensuring privacy in cloud computing that resulted from the Value Focus Thinking phase of this study. The objectives for privacy in cloud computing were derived from interviews with 90 individuals with a wide range of personal and professional experience in cloud computing. We discussed in detail the process of how we performed the analysis of the rich data collected in the interview process of this study. The results of the analysis were presented in a table format listing the 6 fundamental and 19 means objectives that emerged from the study. We provided a detail discussion on the importance of the derived objectives with respect to the extent literature. This discussion established their relevance to the overall strategic objective of ensuring privacy in cloud computing. These objectives will be utilized in the following chapter as the foundation for the development and design of a cloud privacy audit framework.
Chapter 5 Designing a Cloud Privacy Audit Framework

5.1 Introduction

The purpose of this chapter is to design a cloud privacy audit framework. At the core of any design project is the development process or approach used to create the design artifact. For the development of the cloud privacy audit framework we applied the problem-centered approach of the design science research methodology (DSRM) presented by Peffers et al. (2008) while adhering to the seven guidelines for design science research by Hevner et al. (2004). Design science research is concerned with two primary goals. One to design an artifact, Two is to evaluate its utility (Hevner, 2004; March and Storey, 2008). We used the cloud privacy objectives developed in phase one of this study to design a cloud privacy audit framework. According to Simon (1996) design science research focuses on creation of “how things ought to be in order to attain goals and to function” (pp. 4) The framework developed in this phase of the study provides guidance as to what ought to be done to ensure privacy in cloud computing.

The remainder of this chapter discusses the research procedures that we performed during this study. In this chapter we use the six main activities of DSRM to frame the presentation of our design of the cloud privacy audit framework. DSRM incorporates the following process steps: problem identification and motivation, definition of the objectives for a solution, design and development, demonstration, evaluation, and communication. In these sections we discuss the details of the design process of the cloud privacy audit framework and express the rigor of the research performed in each step.
5.2 Problem Identification: Analyzing Privacy in the Cloud

With the rise of cloud computing, critical and sometimes sensitive information that was once safely stored on personal computers now resides on the servers of online companies. The issue with this is that when users allow their information to be stored in the cloud, they lose the ability to maintain complete control of that information (Katzan, 2010). This results in a risk to individuals’ privacy. Dhillon and Kolkowska (2011) have identified privacy as a significant concern in the emerging context of cloud computing. For example one of the risks of storing data in the cloud is the possibility that unwanted third parties will access this data. For example, when email providers allow secondary advertising uses for e-mail communications. Another concern is that cloud users have limited recourse should their data be exposed or lost. This is because the legal rights or regulatory authority over the protection of cloud users’ privacy are not well defined.

Under the Electronic Communications Privacy Act of 1986, data stored in the cloud may be subject to lesser standards than data stored on personal computers (Zhou et al., 2010). This lack of legal privacy protection results in organizations such as Electronic Privacy Information Center or Cloud Security Alliance to champion the legal debate for increasing regulatory controls to protect uses information in cloud computing environments. The World Privacy Forum published a report recently that identified the following cloud privacy concerns: (Gellman, 2009)

- Risks vary significantly with the terms of service and privacy policy established by the cloud provider.
- For some types of information and some categories of cloud computing users,
privacy and confidentiality rights, obligations, and status may change when a user discloses information to a cloud provider.

- Disclosure and remote storage may have adverse consequences for the legal status of or protections for personal or business information.

- The location of information in the cloud may have significant effects on the privacy and confidentiality protections of information and on the privacy obligations of those who process or store the information.

- Information in the cloud may have more than one legal location at the same time, with differing legal consequences.

- Laws could oblige a cloud provider to examine user records for evidence of criminal activity and other matters.

- Legal uncertainties make it difficult to assess the status of information in the cloud as well as the privacy and confidentiality protections available to users.

A primary consideration for cloud users is how do organizations handle personal information and how transparent they are about their information practices. An organization’s integrity and accountability with respect to their information practices is important for ensuring privacy and building user trust (Katzan, 2010). As a means to reduce cloud privacy risks, Pearson and Charlesworth (2009) recommend that organizations use a combination of privacy policies and contractual terms to create accountability in the form of transparent, enforceable commitments towards protecting user’s information privacy. Establishing sound accountability practices in the cloud helps to ensure compliance with regulations and reduce privacy risks (Pearson and Benameur, 2010). We believe that having effective oversight controls of an organization’s privacy practices is paramount to protecting information privacy in cloud computing.
5.3 Objectives of a solution: Creation of a Cloud Privacy Audit Framework

The importance of having strong monitoring and auditing of an organization’s privacy practices has not gone unrecognized by privacy and security professionals. With the rise of data breaches that result in the loss and theft of personal information there is a need to have strong controls in place to protect information privacy. The accounting profession has developed a privacy framework known as Generally Accepted Privacy Principles (GAPP) to help establish guidelines to assess, build, and monitor privacy programs. Cline (2007) describes GAPP as the best attempt so far to address the growing complexity of privacy regulations around the world.

Wang et al. (2010) suggest that performing an audit of cloud providers is important for protecting information privacy in cloud computing. However, traditional audits frameworks do not cover cloud computing-specific security and privacy threats (Dolelitzscher et al., 2013). Audits of privacy practices can mitigate privacy risks and establish trust in a cloud service provider’s processes and practices. Dolelitzscher et al. (2013) argue that in order to provide a secure and trustable cloud environment, audit tasks need to be based on specific knowledge about their environment and cloud-specific characteristics.

Within our process of searching for a suitable privacy framework for auditing cloud computing we soon realized that there is a lack of practical cloud privacy audit frameworks to assist us in the process of formulating audit tasks and performing a cloud privacy audit. For this reason our objective for this design science study is to design a
cloud privacy audit framework. We believed that establishing specific cloud privacy focused audit objectives are an important part of the process to create the cloud privacy audit framework. Hevner (2004, 2007) emphasized the importance that design requirements are gathered from the contextual environment while the theories and methods used to design and evaluate the design artifact are drawn from a known knowledge base. We agree with this philosophy and designed this research study to gather cloud privacy objectives through the rigor application of the value focused thinking approach discussed in the previous chapter. The six fundamentals objectives and the nineteen means objectives for ensuring cloud privacy that were developed in phase one of this study are the building blocks we use as a foundation to develop and design the cloud privacy audit framework.

5.4 Development and design of the Artifact: Constructing a Cloud Privacy Audit Framework

The purpose of this section is to communicate the steps we performed in the process of developing and designing the Cloud Privacy Audit Framework (CPAF). We feel that the CPAF artifact developed in this study meets the two required characteristics, relevance and novelty, of design science artifacts as outline by Geerts (2011). Hevner et al. (2004) proclaims that design science research ought to provide a solution to an unsolved problem in a unique and innovative way or be more effective or efficient. Peffers et al. (2008) agree that solving a current important problem with the design artifact makes it relevant. According to Hevner’s (2007) guidelines the relevance cycle is a conduit between the contextual domain and design activities. The purpose of the
relevance cycle is to integrate design requirements from the problem environment into the design-science study, such that the resulting design-science artifact is effective and relevant to the issues being addressed.

Before the final artifact can be produced it is important that the design process goes though a series of iterations or cycles. Each cycle begins with the building of a design artifact. The artifact is then evaluated, which provides feedback to the design team and researcher to make improvements to the design of the artifact (Peffers et al., 2008). For this iterative process cycle of building and evaluating of the artifact we utilized a focus groups to assist in the design and evaluation processes. For the design phase of this study we utilized an exploratory focus group (EFG) consisting of industry experts with specific cloud experience to evaluate of the design artifact and propose improvements to the design artifact. Tremblay et al. (2010) argue that EFG are useful for achieving improvements in an artifact design when little is known about the phenomenon being study. The newness of cloud computing environments lends itself to the notion that new cloud technology improvements are constantly being rolled out and that limited knowledge is available about the cloud let alone cloud privacy.

As we pointed out earlier in this chapter the design of the artifact started with the cloud privacy objectives (see table 5.1) developed in the VFT phase of this study. We feel our decision to start the design process with the objectives derived from the VFT approach is justified by Geerts (2011) claim that other evaluation methods may be used for early design cycles while focus groups may be used for later cycles of design refinement. During the iterative process of designing the CPAF artifact the
EFG met eleven times over a period of 6 months. Each meeting lasted 90 to 120 minutes depending on the level of engagement and the task the group was working on. The meetings were hosted on WebEx to accommodate group members who were not locally available. This process had the added benefit of being recorded which allowed for a through analysis of each discussion between the design cycles.

Table 5.1 Fundamental and Means Objective for ensuring cloud privacy

<table>
<thead>
<tr>
<th>Fundamental Objectives for ensuring cloud privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>F.O. #1: To increase trust with cloud provider</td>
</tr>
<tr>
<td>F.O. #2: Maximize identity management controls</td>
</tr>
<tr>
<td>F.O. #3: Maximize responsibility of data/asset stewardship</td>
</tr>
<tr>
<td>F.O. #4: Maximize individual’s understanding of cloud service functionality</td>
</tr>
<tr>
<td>F.O. #5: To maximize protection of rights to privacy</td>
</tr>
<tr>
<td>F.O. #6: To maintain the integrity of data</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Means objective for ensuring cloud privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>M.O. #1: To maximize effectiveness of secure data transfers</td>
</tr>
<tr>
<td>M.O. #2: To optimize ease of use of cloud technology</td>
</tr>
<tr>
<td>M.O. #3: To maximize technology infrastructure competencies</td>
</tr>
<tr>
<td>M.O. #4: To have the ability to minimize unnecessary access to information</td>
</tr>
<tr>
<td>M.O. #5: Increase Standardization of cloud technologies</td>
</tr>
<tr>
<td>M.O. #6: To optimize the effectiveness of privacy policy governance</td>
</tr>
<tr>
<td>M.O. #7: To maximize performance of Risk assessments</td>
</tr>
<tr>
<td>M.O. #8: To increase control over information disclosure</td>
</tr>
<tr>
<td>M.O. #9: To ensure CSP has effective HR practices</td>
</tr>
<tr>
<td>M.O. #10: To minimize government access to information</td>
</tr>
<tr>
<td>M.O. #11: To maximize effectiveness of independent oversight of privacy practices</td>
</tr>
<tr>
<td>M.O. #12: To optimize access controls</td>
</tr>
<tr>
<td>M.O. #13: To optimize segregation of information</td>
</tr>
<tr>
<td>M.O. #14: Minimize third party access to information</td>
</tr>
<tr>
<td>M.O. #15: To minimize liability concerns</td>
</tr>
<tr>
<td>M.O. #16: To ensure provider has effective internal controls</td>
</tr>
<tr>
<td>M.O. #17: To maximize availability of cloud resources</td>
</tr>
</tbody>
</table>
The initial task of the EFG was to evaluate the cloud privacy objectives from phase one. The purpose of this process was twofold, first it provided additional validation of the cloud privacy objectives and second it created a level of buy-in and commitment amongst the members of the EFG. This initial task of validating the objectives took three meeting to complete. The first meeting consisted of six EFG members, some of the time were spent introducing everyone and get familiar with each other. A majority of the discussion focused on clarifying definitions, and interpreting the meaning of the identified objectives from the cloud privacy perspective. To help with this understanding we began with a broad explanation of where the CPAF would be beneficial. Followed by a description of how we envisioned the artifact to be and how it might be utilized in the end. We also explained that a CFG would have the ability to utilize and evaluate the CPAF and provide feedback to the EFG about the CPAF’s utility. The second meeting with the EFG members was similar to the first meeting except this time the group had a better understanding of the cloud privacy objectives. With this understanding the group was able to go through each fundamental and means objective in detail and evaluate them and their related sub-objectives to determine their validity and if they provided adequate coverage to ensure cloud privacy. This process incorporated an important resource required for design and development process and that is the industry expertise from a known knowledge base to guide and assist in the development of the design artifact. During the third meeting with the EFG the initial task

<table>
<thead>
<tr>
<th>M.O. #18: Increase awareness of data ownership</th>
</tr>
</thead>
<tbody>
<tr>
<td>M.O. #19: To ensure service contract meets privacy requirements</td>
</tr>
</tbody>
</table>
was completed and resulted in the EFG recommending an additional three means objectives that are presented in Table 5.2 below. The final assessment of these objectives by the EFG resulted in 6 fundamental objectives and 22 means objectives, which are utilized in the development of the design of the CPAF.

Table 5.2 Additional means objectives for cloud privacy

<table>
<thead>
<tr>
<th>M.O. #20: To ensure cloud service providers’ privacy policy and practices are effectively communicated and understood.</th>
</tr>
</thead>
<tbody>
<tr>
<td>M.O. #21: To ensure personal data is removed from cloud host’s infrastructure.</td>
</tr>
<tr>
<td>M.O. #22 To maximize performance of vulnerability assessments</td>
</tr>
</tbody>
</table>

The second task of the EFG during the design phase of the CPAF was to develop a means and fundamental relationship matrix that represented which means objectives supported the goals of the stated fundamental objectives. In order to develop this matrix each member of the EFG was requested to individually complete a matrix check lists. In this process they identified the means objectives that they felt strongly supported a fundamental objective with a number one and then identified means objectives that they felt somewhat supported a fundamental objective with a number two. Once all six members of the EFG completed this task we reconvened to discuss the reasons and rational each member had in linking a specific means objective to a specific fundamental objective. The final means and fundamental relationship matrix is presented in table 5.3 below. For the purpose of this matrix we felt that it was still important to include the weaker relationships with the stronger ones on the final matrix. This purpose behind this step was to identify what means objectives supported the state purposes and aims of
each fundamental objective. This matrix provided the foundation that brought the individual means and fundamental objectives together to form the CPAF presented in the next iterations of the design process, and also the final version that is present in the demonstration phase.

Table 5.3 Means and Fundamental relationship matrix

<table>
<thead>
<tr>
<th>Mean and Fundamental Objective linkage matrix</th>
<th>F.O. #1: To increase trust with cloud provider</th>
<th>F.O. #2: Maximize identity management controls</th>
<th>F.O. #3: Maximize responsibility of data/asset stewardship</th>
<th>F.O. #4: Maximize individual’s understanding of cloud service functionality</th>
<th>F.O. #5: To maximize protection of rights to privacy</th>
<th>F.O. #6: To maintain the integrity of data</th>
</tr>
</thead>
<tbody>
<tr>
<td>M.O. #1: To maximize effectiveness of secure data transfers</td>
<td>2</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M.O. #2: To optimize ease of use of cloud technology</td>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M.O. #3: To maximize technology infrastructure competencies</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M.O. #4: To have the ability to minimize unnecessary access to information</td>
<td></td>
<td>1</td>
<td>1</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>M.O. #5: Increase Standardization of cloud technologies</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>M.O. #6: To optimize the effectiveness of privacy policy governance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M.O. #7: To maximize performance of Risk assessments</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>M.O. #8: To increase control over information disclosure</td>
<td></td>
<td>1</td>
<td>1</td>
<td></td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>M.O. #9: To ensure CSP has effective HR practices</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M.O. #10: To maximize government access to information</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M.O. #11: To maximize effectiveness of independent oversight of privacy practices</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M.O. #12: To optimize access controls</td>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M.O. #13: To optimize segregation of information</td>
<td></td>
<td></td>
<td></td>
<td>2</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>M.O. #14: Minimize third party access to information</td>
<td></td>
<td>2</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M.O. #15: To minimize liability concerns</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>M.O. #16: To ensure provider has effective internal controls</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>M.O. #17: To maximize availability of cloud resources</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M.O. #18: Increase awareness of data ownership</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M.O. #19: To ensure service contract meets privacy requirements</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M.O. #20: To ensure cloud service providers’ privacy policy and practices are effectively communicated and understood</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>M.O. #21: To ensure personal data is removed from cloud host’s infrastructure</td>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M.O. #22: To maximize performance of vulnerability assessments</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The third task for the EFG was to consider the priority of the means objectives that the group decided was linked to supporting the goal of the fundamental objective. During this process the EFG first individually ranked the importance of the means objectives for each fundamental objective. Then the group reconvened as a whole to determine which means objectives was the most important for ensuring the fundamental objective being assessed. For example table 5.4 represents the ranking of the means objectives that support the end goal of the fundamental objective to increase trust with the cloud provider.

Table 5.4

<table>
<thead>
<tr>
<th>F.O. #1: To increase trust with cloud provider</th>
<th>Rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>M1 To maximize effectiveness of secure data transfers</td>
<td>1</td>
</tr>
<tr>
<td>M.O. #20: To ensure cloud service providers’ privacy policy and practices are effectively communicated and understood.</td>
<td>2</td>
</tr>
<tr>
<td>M.O. #16: To ensure provider has effective internal controls</td>
<td>3</td>
</tr>
<tr>
<td>M.O. #15: To minimize liability concerns</td>
<td>4</td>
</tr>
<tr>
<td>M.O. #6: To optimize the effectiveness of privacy policy governance</td>
<td>5</td>
</tr>
<tr>
<td>M.O. #7: To maximize performance of Risk assessments</td>
<td>6</td>
</tr>
<tr>
<td>M.O. #11: To maximize effectiveness of independent oversight of privacy practices</td>
<td>7</td>
</tr>
<tr>
<td>M.O. #17: To maximize availability of cloud resources</td>
<td>8</td>
</tr>
<tr>
<td>M.O. #10: To minimize government access to information</td>
<td>9</td>
</tr>
<tr>
<td>M.O. #9: To ensure CSP has effective HR practices</td>
<td>10</td>
</tr>
<tr>
<td>M.O. #22: To maximize performance of vulnerability assessments</td>
<td>11</td>
</tr>
</tbody>
</table>

After the EFG agreed upon the rankings of the means objectives within each category of fundamental objectives we determined, which means objectives, would be
included in the initial design of CPAF. In the example noted above the EFG determined that the first six ranked means objectives needed to be included in the framework. Please refer to version one of the CPAF presented below.

**Version 1 of the Cloud Privacy Audit Framework (CPAF)**

1. **Increase trust with cloud provider**
   - Maximize effectiveness of secure data transfers
   - Ensure cloud service providers’ privacy policy and practices are effectively communicated and understood.
   - Ensure provider has effective internal controls
   - Minimize liability concerns
   - Optimize the effectiveness of privacy policy governance
   - Maximize performance of Risk assessments

2. **Maximize identity management controls**
   - Have the ability to minimize unnecessary access to information
   - Increase control over information disclosure
   - Optimize access controls

3. **Maximize responsibility of data/asset stewardship**
   - Have the ability to minimize unnecessary access to information
   - Increase control over information disclosure
   - Minimize third party access to information
   - Ensure provider has effective internal controls
   - Increase awareness of data ownership

4. **Maximize individual’s understanding of cloud service functionality**
   - Ensure service contract meets privacy requirements
   - Ensure cloud service providers’ privacy policy and practices are effectively communicated and understood.

5. **Maximize protection of rights to privacy**
   - Have the ability to minimize unnecessary access to information
   - Minimize liability concerns
   - Maximize effectiveness of independent oversight of privacy practices

6. **Maintain the integrity of data**
   - Ensure provider has effective internal controls
   - Increase control over information disclosure
   - Optimize segregation of information
   - Maximize effectiveness of secure data transfers
Once this initial version of the CPAF was completed the results were shared with the CFG as a means to evaluate it. In order to ensure the CFG understood the design process that resulted in the development of the CPAF, we communicated the steps performed by the EFG in tasks one, two and three. Since the CFG was utilized to evaluate the cloud privacy objectives in the VFT phase of this research study they were already very familiar with them. During the evaluation process they agree with the means and fundamental relationship matrix however they believed several key means objectives were not included in the original version of the CPAF.

The following were the objectives the CFG believed needed to be included in the CPAF. Under F.O. #1: To increase trust with cloud provider they felt that it was important to include M.O. #11: To maximize effectiveness of independent oversight of privacy practices. Under F.O. #2: Maximize identity management controls there were two objectives they thought need to be included. M.O. #1: To maximize effectiveness of secure data transfers and M.O. #16: To ensure provider has effective internal controls. Under F.O. #3: Maximize responsibility of data/asset stewardship they felt it was important to include M.O. #7: To maximize performance of Risk assessments. Under F.O. #4: Maximize individual’s understanding of cloud service functionality they felt it was important to include M.O. #8: To increase control over information disclosure. Under F.O. #5: To maximize protection of rights to privacy they felt it was important to include M.O. #19: To ensure service contract meets privacy requirements and M.O. #10: To minimize government access to information. Under F.O. #6: To maintain the integrity of data they felt it was important to include M.O. #22: To maximize
performance of vulnerability assessments.

Going through an evaluation process such as this allowed us to determine whether or not additional iterations of the design cycle are needed to effectively solve the problem being addressed. Based on this initial evaluation of the CPAF by the CFG it was determined that another iteration of the design cycle would be required. The EFG was brought back together and provided the feedback from the initial evaluation of the CPAF artifact performed by the CFG. Based on this feedback and additional debates amongst the EFG members some of the recommendations from the CFG were added to the framework. In addition, the EFG believed a few other means objectives were overlooked in the initial version of the CPAF and in the CFG recommendations and decided to add them to the final version of the CPAF. The final version of the CPAF artifact is presented in the next section.

5.5 Demonstration of the Cloud Privacy Audit Framework

This step demonstrates the use of the CPAF and its ability to solve the need to ensure cloud privacy within a real cloud environment. To demonstrate the general applicability of the CPAF for the audit planning process we utilized an existing audit team that performs information system security audits as a CFG. The audit team works for a state agency and performs audits on 86 state agencies with wide range operational and regulatory requirements related to protection of privacy. This team explained that the majority of their audit function is to ensure financial data is accurately being report to the state legislator and its citizens. However, they also reported that many of the
entities they audit also contain sensitive personal, financial, and health related
information that needs to be protected as well through extensive privacy and security
audits. The final version of the CPAF presented below was shared with the CFG for
their analysis of its utility and ease-to-use and to compare to existing generally accepted
accounting principles (GAPP).

Cloud Privacy Audit Framework

1. Increase trust with cloud provider
   • Maximize effectiveness of secure data transfers
   • Ensure cloud service providers’ privacy policy and practices are effectively communicated and understood.
   • Ensure provider has effective internal controls
   • Minimize liability concerns
   • Optimize the effectiveness of privacy policy governance
   • Maximize performance of Risk assessments
   • Maximize effectiveness of independent oversight of privacy
   • Maximize availability of cloud resources

2. Maximize identity management controls
   • Have the ability to minimize unnecessary access to information
   • Increase control over information disclosure
   • Optimize access controls
   • Maximize effectiveness of secure data transfers

3. Maximize responsibility of information stewardship
   • Have the ability to minimize unnecessary access to information
   • Increase control over information disclosure
   • Minimize third party access to information
   • Ensure provider has effective internal controls
   • Increase awareness of data ownership

4. Maximize individual’s understanding of cloud service functionality
   • Ensure service contract meets privacy requirements
   • Ensure cloud service providers’ privacy policy and practices are effectively communicated and understood.
   • Increase control over information disclosure
5. Maximize protection of rights to privacy
   • Have the ability to minimize unnecessary access to information
   • Minimize liability concerns
   • Maximize effectiveness of independent oversight of privacy practices
   • To ensure service contract meets privacy requirements

6. Maintain the integrity of data
   • Ensure provider has effective internal controls
   • Increase control over information disclosure
   • Optimize segregation of information
   • Maximize effectiveness of secure data transfers
   • Maximize technology infrastructure competencies

In this demonstration process of the CPAF the audit team assessed the completeness and applicability of the framework in their work environment. The testing process went through several iterations until the audit team felt that the cloud privacy audit framework was an effective tool from which they could develop a high quality audit work program for auditing cloud privacy. The discussion about the evaluation of the final iteration of the CPAF presented here and its utility will be presented in the next section.

5.6 Evaluation: Findings and limitations of the Cloud Privacy Audit Framework

This section reports and discusses the results of the evaluation. The goal of this step is to assess how well the design artifact can resolve the defined research problem (Peffers et al., 2008). The major type of data collected for evaluation is qualitative data through in-depth discussions with a confirmatory focus group, with complementary data from individual questionnaire from group members. Confirmatory Focus Groups are a good way to evaluate the utility and applicability of the artifact design in the contextual environment (Tremblay et al., 2010). The use of CFG allows for flexibility, direct
interaction with respondents, collection of large amounts of rich data, to build on other respondent’s comments (Stewart et al., 2007). For the CFG we utilized an existing audit team with six members because of their expertise and knowledge of IS auditing.

During the evaluation we presented the final version of the cloud privacy audit framework to the group of auditors. We explained the rational of the changes we have made to the list of objectives within the framework. We explained that the intention of the cloud privacy audit framework was to assist them in their audit planning process to ensure that they coverage of all the primary privacy risks associated with cloud computing. As a means to stimulate individual clarity we had group members individually document their impressions as to the relevance and usefulness of the framework as it would relate to planning an audit of a system that utilizes cloud technology. Once everyone was satisfied they had documented there own opinions on the framework we had an open discussion on how they believed the CPAF would be used in their organization and how it could be incorporated into their normal audit work processes.

The process of bringing the designed artifact into the environmental context for which it was designed and evaluated to ensure that it does indeed work is an important component of the relevance cycle (Hevner, 2007). Evaluating the artifact in the field allows researchers to determine whether or not additional iterations of the design cycle are required to effectively solve the problem being addressed. In this study the process of testing the cloud privacy audit framework is achieved by having an information security audit team assess the completeness and applicability of the cloud
privacy audit framework in their work environment. The CFG was involved with the
evaluation of the design artifact at three different intervals of the design process. Initially
the CFG was consulted on their opinions of the means and fundamental objectives that
were to be included in the design process of the CPAF. In the second phase of the design
process the CFG evaluated the relationships matrix between the fundamental and means
objectives. They also provided feedback as to what means objectives they viewed as
being important in ensuring the related fundamental objective was met. In the final
iteration of the evaluation process the CFG evaluated the final CPAF as it was presented
in step four. The CFG recommended several changes throughout this process. We have
already discussed these recommendations in the development and design section of this
chapter so we will not discuss them again here. The rigor of this research is
communicated by the fact that several iterations were performed until the audit team felt
that the cloud privacy audit framework was an effective tool from which they could
develop a quality audit work program for auditing cloud privacy.

5.6.1 Perceived Usefulness and perceived ease-of-use of Artifact

The qualitative data from the CFG provides rich evidence that the design
objectives are basically satisfied. In this section we present the CFG’s opinions about the
CPAF and its ability to meet the high-level design objectives of utility and ease-of-use.
For discussion purposes we have also included group members concerns with certain
aspects of the framework.
5.6.1.1 Perceived Usefulness (utility)

The biggest advantage of the framework is that it provides greater detail as to what considerations need to be included in the audit process to ensure privacy than other privacy frameworks do, such as GAPP. The CFG members generally agreed that the CPAF is useful in providing guidance as to what need to be covered in their audit programs and that it could be helpful to them in their planning process. An analysis of the members’ responses reveals how they perceived the CPAF to be useful. One of the audit team members made the following statement:

“In my opinion, yes the CPAF is useful. To date there is no established framework to develop and implement audit program steps specifically for cloud computing. When we do encounter an agency that utilizes a cloud solution, we rely on the SOC report to determine reasonability that controls are in place and monitored. I feel that this framework would be beneficial to an IS auditor.”

The audit team also expressed how they felt the increased level of detail in the CPAF would be useful to them. Here are a few examples of their comments during the evaluation of the utility of the CPAF. One CFG member stated that

“The CPAF will provide a more detailed framework relating to cloud privacy that I do not believe exists today. It will help in defining detailed control objectives in our audit programs that ensures sufficient coverage in order to keep our audit risk low. While some of the minor objectives are already covered as part of our test work, I see many that are not, and based on a risk environment approach may be important to include in the work.”

Other CFG members also described how they felt the framework would be useful to them.

“It would work well in the IS audit space. Using the fundamental objectives as a guide for what aspects of cloud privacy we should look into.”

“It would be useful, especially with regard to the CPAF areas of availability and customer understanding of functionality. The GAPP does not necessarily address those areas.”

While the majority of the feedback from the CFG was positive with regards to CPAF
usefulness there were some concerns expressed as well such as the following in regards to the trust objective outlined in the CPAF.

“My only reservation would be the “Increase Trust” aspect of the framework which seems subjective and subjects the auditor to too much “judgment”.

“Trust is a difficult objective to audit, but very important. The sub-objectives will provide adequate tools to look into in order to verify the trust.”

Another CFG member in the following statement addressed these concerns:

“In terms of audit standards and audit process what we include comes down to audit risks. Our whole audit planning process is that we want to keep our audit risks to be low, no matter what. When we issue a report having a low audit risk we ensure trust. Meaning that if we have a high audit risk then who ever is reading the report can not put a lot of trust into it. Meaning we did not have enough coverage, we did not design out test work to cover enough stuff to give it a high level of competence to what we are saying, if are saying controls are good, that they can trust that, or if we are saying controls are bad, that they can trust that. So we want to keep audit risks levels low at all times. This framework provides guidance on how we can ensure enough coverage during our planning process.”

It is important to note that the CPAF is not intended to be a privacy audit work-program that can be immediately picked up and completed to perform an audit of cloud privacy. Its purpose is to provide additional and complementary perspective to the audit planning process. In this regards CPAF has been found to be very effective and useful to the audit team members.

5.6.1.2 Perceived Ease-of-use

Utility is not the only evaluation objective of this approach. It has to be easy to use as well to ensure that it will be adopted. Several of the CFG members’ noted the following:

“I feel that it would be relative easy to incorporate the CPAF into our process. The CPAF touches on many aspects that are not present today”

“It would be fairly easy to incorporate in to our audit planning process. The minor objectives described in the CPAF will allow a more compressive scope for auditing cloud
privacy.”

“These are clear privacy objectives, allowing the framework to be easily adopted into an audit program.”

“Relative easily. We would select appropriate sub objectives to cover each means objective, this would provide guidance for accurate coverage”

While the majority of the comments are encouraging that the CPAF could be easy to implement into an audit team’s planning process there were a couple concerns expressed about the adoption and implementation of the framework. The following statements were made:

“I do fear, however, that the repeat objectives might be confusing when attempting practically implement a program.”

“Sometimes details can be your enemy when evaluating a system of internal controls as you may miss the 30,000-foot view and any issues there.”

These comments are helpful in how to ensure ease-of-use with respect to adoption of the CPAF. The purpose of the framework and how to use it as a guiding audit tool needs to be communicated clearly in order to increase the understanding of how to use it. For example, how would it be used the development of the audit scope to ensure it covers enough areas of concern to protect cloud privacy. A good summary of how the CPAF meets the design objectives of increasing utility and ease-of-use and be summed up by a statement from the audit teams director provided that seemed to summarize everyone’s view.

“I think that these objectives that are on here will help compliment the programs that we have. We indirectly audit a cloud service provider right now, which is NG, which offers cloud infrastructure services to the commonwealth. We do this by in part going to each agency and auditing the way they design their security and privacy programs, as well as their applications and how they develop those. We don’t touch their infrastructure we rely on Deloitte’s report on the infrastructure to give us coverage over the infrastructure part. But when we are looking at for example, web applications that is available to the citizens in order for them to them, and the fact that all these applications run on a single network now, this cloud service network, I think looking at these objectives will complement what we done so far in that it will help to ensure we have focused our coverage on the right stuff. I think going through this exercise
process and looking at all these objectives will help us to fine tune our audit programs and audit processes as we go into these agencies and look at what we will audit.”

An analysis of the qualitative data and the CFG viewpoints covered here are positive evidence that the evaluation of the CPAF has clearly shown it’s utility and ease-of-use in the context of ensuring cloud privacy. We feel that the evaluation process of the CPAF performed here meets the requirements of relevance as expressed by Hevner (2004, 2007).

5.7 Communication of the Contribution of the Design Science Study

The purpose of this step is to communicate the importance of ensuring cloud privacy and how our designed artifact, CPAF, is an innovative solution to the problem, the rigor of its design process, and the effectiveness of it’s contribution to researchers and practitioners. We believe we have contributed to the body of knowledge and have provided a valid piece of design research according to Hevner et al. (2004)’s seven guidelines. We met the requirements of guideline 1 - design an artifact: by creating an innovative and purposeful artifact for the audit planning process of ensuring cloud privacy. Our study meets the requirements of guideline 2 - problem relevance: due to the recent concerns towards the rapid expansion of cloud technologies and the lack of the development of ethical privacy standards and regulations our research proves to be very relevant to the domain of cloud computing. We met the requirements of guideline 3- design evaluation: by utilizing a real audit team as a confirmatory focus group to evaluate the utility and ease-of-use of the CPAF. Our research met the requirement for guideline 4-research contribution: by making the cloud privacy audit planning process
more effective, efficient and detailed focused than it been before. We have met the requirement of Guideline 5 – research rigor: by rigorously designing and demonstrating and evaluating the CPAF through multiple iterations and by applying the design science research methodology (DSRM) (Peffers et al. 2008). We meet guideline 6 – design as a search process: by utilizing a VFT approach to develop cloud privacy objectives to define the requirement for the CPAF. We are meeting the requirement for guideline 7 – communication of research: by the writing and defending this dissertation. In addition the application of the Keeney’s (1994) VFT approach within the design science research methodology (Peffers et al. 2008) is in itself a contribution to the philosophy of IS and design science research debate.

5.8 Summary

This chapter presented the Cloud Privacy Audit Framework as a design artifact that was developed through a rigorous application of the Design Science Research Methodology as recommended by Peffers et al. (2008). During application for this methodology it is important that the researcher utilizes theories, methods, industry expertise from a known knowledge base to guide and assist in the development of the design artifact. The development of a rigorously designed research artifact is a continuous process that includes elements of design, relevance and rigor intertwined together. This process is also an iterative process because as new issues emerge in the development of the design artifact the researcher needs to back existing knowledge base to determine what methods or tools he/she should use or apply to resolve the new design problem. For the purpose of this study we have extensively use the IS and
accounting literature to provide guidance for the design of a cloud privacy audit framework. For each iteration cycle of the CPAF design artifact we referenced the existing knowledge base to find known solutions or to provide guidance as to how to proceed in the next step of the design. A good design science research study will contribute to both the environment and its informing knowledge base (Hevner 2007). It is our belief that one of this study’s contribution back to the knowledge base is through the use of a Value Focused Thinking approach as a means to define design objectives in the application of the Design Science Research Methodology. Another contribution to the knowledgebase will be the Cloud Privacy Audit Framework itself. These contributions will be discussed in greater detail in chapter seven.
Chapter 6 Discussion

6.1 Introduction

The purpose of this chapter is to provide a synthesis of this study and to make insightful connections between this study’s findings and the existing knowledge base. A synthesis is the combination of parts or elements so as to form a whole. This is where we contemplate the implications of our research findings. The findings of this research study have been presented in previous chapters; however, they are brought together here again for a more in-depth discussion as to their implications for managing information privacy in cloud computing.

Managing privacy in the cloud is a challenge because organizations must not only meet internal privacy requirements but they must also deal with external requirements such as privacy regulations in multiple jurisdictions. Culnan and Armstrong (1999) argue that ensuring systems are compliant with legal privacy regulations requires a multidisciplinary approach. This is because it requires cooperation from key information professionals throughout the organization. IT specialists design and build the systems handling personal information. Information security specialists ensure the systems protect the storage, processing, and transmission of data. Privacy officers and the corporate lawyers develop privacy policies to ensure the organization is compliant with all the privacy laws of the jurisdictions in which they operate. Information systems auditors inspect privacy policies and practices to ensure compliance is maintained. Orchestrating all these processes simultaneously requires an
organization’s privacy management team to have an expertise in the following three areas of cloud privacy management; forming a cloud privacy strategy, evaluating cloud privacy practices, and auditing of cloud privacy. The remainder of this chapter will discuss the importance of these key functions areas for ensuring information privacy.

6.2 Cloud Privacy Strategy

The concept of strategy has often been described as managerial processes such as planning and control, defining mission and purpose, identifying and allocating resources to achieve an organization’s objectives (Dhillon, 1995). Strategic planning has been positively linked to performance, implementing change successfully, and decision success (Hutzschrenereuter & Kleindienst, 2006). Despite the importance of information privacy in organizations today (see Culnan and Armstrong, 1999; Smith et al, 1996) our extensive review of the literature suggests that the concept of a privacy strategy has not been investigated very much by IS privacy researchers. There is a bit of uncertainty as to what makes up a privacy strategy in the privacy literature. Even in the main steam IS literature the concept of IS strategy is somewhat vague. For example, Chen et al. (1997) define it through its connection to business strategy, and Henderson and Venkatraman (1999) consider it to be an independent strategy within the organization. Dhillon (1995) noted that there is often confusion between what is designated as a policy and what is an IS security strategy. For the purpose of this discussion we define strategy as a shared organizational perspective on setting and meeting organizational goals (Chen et al., 2010). Using this as a foundation we define an information privacy strategy as a shared organizational perspective on setting and meeting an organization’s
information privacy goals.

6.2.1 Strategic Planning for Cloud Privacy

Strategic privacy planning requires management to consider how they can gain competitive advantage through the collection and use of transaction data, and limit the downside risk of such activities. Glazer (1991) found those organizations that use transaction data as an organizational resource can create benefits for both consumers and the organization such as better customer service, higher quality products, and new products that reflect consumer preferences. The collection of detailed personal information also allows organizations to engage in relationship marketing in the hopes of increasing future sales (Blattberg and Deighton, 1991). However these practices also raise privacy concerns and may lead to customers being unsatisfied with their experience and to lose trust in the organization’s ability to protect their information. This could result in a negative impact on the bottom line through customer defections, bad word of mouth and the difficulty of attracting new customers.

Jones (1991) argued that firms would find it hard to compete on privacy protection because it is considered negative information. However, with the surge in the number of identity thefts and other privacy violations this view of privacy having no strategic benefit is no longer valid. Ashworth and Free’s (2006) argue that privacy protection can be a strategic asset. Bowie and Jamal (2006) found that firms that are considered to be “safer” or “trustworthy” with respect to privacy are likely to have a competitive advantage. There is a growing consensus among the information privacy
research community that the protection of information privacy can be utilized to create a competitive advantage through strategic planning. However, few organizations are taking advantage of this strategic opportunity, Sarathy and Robertson (2003) found that most firms simply react and adapt to regulatory, industry or consumer pressures regarding consumer privacy. Instead of being reactionary organizations need to develop an approach to proactively manage privacy protection as a strategic option.

A challenge for management in the development of a cloud privacy strategy is to find a balance between two opposing strategic objectives, increasing profits or increasing customer loyalty. One way to increase profits is through selling or using customer’s personal information to market additional goods and services to them. Organizations that behave responsibly and have strong ethical privacy practices create goodwill with their customers. These practices create a loyal customer base, which lowers the cost of doing business. Having a well-defined cloud privacy strategy helps management communicate their intentions towards protecting their customer’s privacy and creating long-term relationships with their customers. In order to form a long term relationship individuals have to trust that their cloud service provider has their best interest at heart. The connection between trust and privacy has been examined in the information systems literature from multiple perspectives. Fukuyama (1995) describes trust has an essential element for sharing information. Metzger (2004) also found trust to be strongly related to information disclosure. In essence, individuals are willing to share or grant access to information only after they have attained a certain level of trust. Therefore, building consumer trust in an organization’s privacy practices should be a
Strategic planning is a activity or process that helps to reduce uncertainty, organize the actions of organizational members, open lines of communication and proactively search for opportunities to create a competitive advantage (Segars and Grover, 1999). It has been suggested that strategic planning for information systems is similar to main-stream organizational strategic planning processes found in strategic management literature (Chan et al. 1997, Henderson and Sifonis 1988, Hufnagel 1987, Venkatraman 1985) and therefore, should be operationalized in similar terms. Segars and Grover (1999) used a conceptualization approach suggested by Earl (1993) to analyze the nature of planning profiles to gain an understanding of strategic planning for information systems. From this analysis Segars and Grover (1999) identified six broad process dimensions that are useful in the operationalization of an information systems strategic planning process. These dimensions are comprehensiveness, formalization, focus, flow, participation, and consistency. With the rapid growth of cloud technology adoption there is a need for organizations to focus on the development of an information privacy strategy. The following section will consider these dimensions as they apply to the development of an information privacy strategy for cloud computing.

6.2.2 A synthesized perspective on the development of a cloud privacy strategy

Top corporate executives have long identified improving strategic planning within the realm of information technology management as a critical competitive issue (Segars and Grover, 1999). In their attempt to better understand the process of
developing a privacy strategy Sarathy and Robertson (2003) considered the influence of the firm's national historical and cultural context, the legal environment, and its ethical philosophy and found them to be important to the development process of a privacy strategy. These findings suggest that an organization’s values are important component in the privacy strategy formulation process. Ghamdi (2005) argues that the use of strategic planning tools and techniques are required for organizations to be effective in their planning process. For the purpose of this synthesis we utilized the identified cloud privacy objectives from our study and Segars and Grover’s (1999) six dimensions as a framework to discuss the contextual process of creating a cloud privacy strategy.

6.2.2.1 Comprehensiveness

With regards to strategic planning process comprehensiveness refers to the extent of the search for a solution. Fredrickson (1984) emphasized the strategic importance of being comprehensive in making and integrating decisions. The concept of comprehensiveness being an important construct in strategic planning has been well established. Janis and Mann (1977) determined that comprehensiveness is composed of several behavioral characteristics such as: thoroughly researching a wide range of alternatives, evaluating a broad spectrum of objectives, constantly weighing the risk/benefit of various consequences, intensively searching for information to objectively evaluate alternative actions, seeking expert judgment regarding alternative actions. With respect to being comprehensive in the formulation of a cloud privacy strategy it is important that an organization consider all consequences of their
information handling practices.

The cloud privacy objectives identified in this study can be used as a strategic planning tool by an organization to ensure that they are being thorough in their considerations of their privacy practices. For instance one privacy objective noted in the study is that individuals wish to increase control over information disclosure. Depending on the cloud service providers’ revenue model they may need to sell the information they collect about their users to third parties. If an organization intends to sell data to a third party they can adhere to several different strategic options that impact users privacy. In one case companies can keep their intentions to sell private data a secret, much like Facebook did during its early days. However, this approach is very often just a short-term strategy to maximize profits, because eventually users will stop using the cloud services when they find out. A second option is to offer customers the ability to opt out, which implies that the company will sell users data to a third party unless the users opt out of this process. This is an option many Internet and cloud providers are including in their privacy strategy. This is because while it provides transparency to the users as to the intentions of the company’s privacy practices, it requires action on the part of users to protect their information. A third strategic option is to provide users with the ability to opt-in and share their information with a third party. This strategic option is probably the least used but it provides users the highest level of control over the disclosure of their information. All three options are valid privacy strategies. However, the privacy regulatory requirements, potential revenue stream, and the impact to consumer trust compared to the organization’s corporate strategy will determine which strategic option
is best.

This level of completeness or comprehensiveness needs to be applied to all aspects of the cloud privacy strategy planning process. Each cloud privacy objective needs to be exhaustively evaluated based on its costs and benefits before making any strategic decisions as whether or not to incorporate the privacy objective into their privacy practices or policies. Essentially, organizations must balance the benefits to their privacy practices with the costs of inaction, human capital, and financial resources by performing a thorough decision analysis process.

6.2.2.2 Formalization

Another distinct process characteristic identified with strategic planning is formalization, which is the existence of rules and procedures that guide the planning process. Segars and Grover (1999) claimed that highly formal planning systems provide a more efficient process for constructing strategic plans. These formal planning systems are characterized by written policies that define the structure and outline formalized techniques for conducting strategic planning. Having a formalized process for developing and review a privacy strategy produces efficiency gains for both the receipt and processing of information.

Establishing a level of formalization towards privacy was included in several of the cloud privacy objectives that could be used in the strategic planning process for developing a privacy strategy. One such objective was to maximize performance of risk assessments. Having a well-documented process for performing privacy risk
assessments would help the strategic planning process for developing a privacy strategy by identifying threats to information privacy thereby providing management with the opportunity to develop a strategy as to how to address the privacy threat. Another cloud privacy objective that supports a formal process for strategic privacy planning is to ensure the cloud service provider’ privacy policies and practices are effectively communicated and understood. This would require that privacy policies and practices to be documented such that they can be shared and communicated with various stakeholders. A common policy requirement of any policy is to incorporate an annual review process to ensure that the documented policy maintains its relevancy. Therefore, the privacy policy itself would be a good place to outline the formal procedures for developing a privacy strategy.

6.2.2.3 Focus

A third strategic planning process identified by Segars and Grover (1999) is that of focus. Chakarvarthy (1987) refers to focus, as the balance between creativity and control measures that are inherent to the strategic planning process. Control measures for strategic planning process can be defined through strict accounting and budgeting practices, which are designed to analyze strategic resource allocation. Creativity has been expressed as the process of generating ideas through entrepreneurial innovation. Such innovation includes idea-generating activities such as systematically evaluating external competitive environments to identify threats or opportunities (Segars and Grover, 1999). When a strategic opportunity as been identified in the strategic planning process it needs to be analyzed as to its possible fit with an organizations
overall strategic plan. During this process, management evaluates corporate resources to assess corporate readiness before attempting to integrate the strategic opportunity into their strategic plan. Having a level of focus in the strategic planning process allows management to maintain a clear vision as to how to implement their strategic goals.

Cloud service providers can benefit from incorporating an element of focus in their strategic planning process. With the constantly changing environment that exists in the cloud-computing domain it is important that organizations are constantly reviewing their information privacy practices. This includes being aware of any privacy regulation changes being proposed in the jurisdictions in which they operate. In addition, an organization needs to constantly be reviewing new technologies being developed which could either propose a threat or an opportunity to their systems infrastructure with respect to protecting information privacy. This continuous scanning of the technology environment will encourage creativity and innovation within an organization. However it is also important to note that controls need to be in place such as a formal cost-benefit analysis to ensure capital resources are not being frivolously allocated whenever a cool new technology is developed. Creating a corporate culture that supports an element of focus within the strategic planning process helps to ensure that an effective and executable cloud privacy strategy is developed.

6.2.2.4 Flow

Another strategic planning process espoused by Segars and Grover (1999) is that of flow, which addresses the vertical orientation of the strategic planning system.
Chakravarthy (1987) describes flow as the devolution of responsibilities. Typically in strategic planning there are two types of flow, “top-down” where the planning process flows from top management to lower levels in the organization or “bottom-up” where the planning process flows from lower levels of management to higher corporate levels. A top-down approach is characterized by limited participation by lower-level managers in the strategic formulation process. As a result, the implementation of the strategic goals by lower-level managers can be challenging due to the post hoc nature of this flow. Whereas a bottom-up approach to strategic planning incorporates a high degree of functional management involvement in the initiation of the strategic planning process. Here the responsibility of top management is to facilitate the strategic planning process by evaluating and organizing the ideas and proposals submitted by lower management into an overall plan for the organization. Either approach can be effective depending on the organizational structure of a company.

Organizations utilizing cloud technologies need to be cognizant of how the formalization of their information privacy strategy is developed. While a “top-down” perspective may be effective for ensuring strong governance over privacy policies however it may not be the best approach for identifying strategic privacy objectives in cloud computing environments. Because of dynamic nature of cloud computing, operational managers may be in a better position than top management to identify vulnerabilities in the system, which could pose a threat to the protection of information privacy. An effective option for developing a cloud privacy strategy is to ensure that both “top-down” and “bottom-up” flows are incorporated into the strategy planning
process. This can be achieved by having strategic planning meetings once a quarter where the chief privacy officer or the lead manager responsible for developing a privacy strategy meets with key operational managers to get a sense for any developing privacy concerns or issues. Additionally, the privacy manager needs to be included in the strategic meetings involving the development and use of information technologies so that others involved in the development of strategic goals for the organization are better informed as the risks or opportunities with respect to information privacy.

6.2.2.5 Participation

The fifth dimension of a strategic planning process identified is participation, which addresses the breadth of involvement in the strategic planning process (Segars and Grover, 1999). Strategic planning structures that support a narrow level of participation or involvement among operational team members is associated with a “top-down approach to planning (Byrd et al. 1995) and tends to result in a limited view towards strategic development. While this may be an acceptable approach when there is limit business expertise at lower levels in an organization however the nature of the cloud-computing environment is not conducive to this type of approach. This is due to the instability and number of issues that are still being addressed in cloud computing. A broader participation approach that includes team members from multiple functional and operational areas in the strategic privacy planning process may be more beneficial in cloud computing environments. This approach helps to reduce the likelihood of "bounded rationality" by top managers when they are inundated by the complexity of cloud computing environment.
6.2.2.6 Consistency

The final dimension of strategic planning noted by Segars and Grover (1999) is that of the frequency of planning otherwise known as consistency. This dimension incorporates the frequency of strategic planning activities such as evaluation or revision of strategic choices, which are important to ensure strategic adaptability (Kukalis, 1991). Strategic planning structures with high levels of consistency are known to have continuous planning processes with frequent meetings for the assessment and revision of their strategic direction. Sabherwal and King (1995) suggest that high consistency planning processes increase the speed an organization makes a strategic decision. A high level of consistency in the strategic planning process would also help to facilitate a rapid adaptation to unexpected changes in external privacy regulations. For developing a cloud privacy strategy it is important to encourage a high level of consistency in the strategic planning process.

6.2.3 Summary

This purpose of this section was to provide a foundation for developing a cloud privacy strategic plan. Important concepts and process dimensions that are important in the formulation of effective strategic planning processes are reviewed. All of the process dimensions discussed in this section are well grounded in the strategic management literature and provide key insights into understanding how and why planning occurs within the organization. Knowledge of these planning process dimensions and along with an understanding of their implications within the scope of the rapidly changing
environment of cloud computing can help facilitate an alignment between a company’s cloud privacy strategy and their higher-level strategic goals.

6.3 Evaluation of Cloud Privacy Practices

Winston Churchill made a profound statement that can be applied to any strategic situation, he said “However beautiful the strategy you should occasionally look at the results.” The business environment is never static, it is in a constant state of change, and therefore organizations should review their operations periodically to ensure their strategic goals are still the same and they are being achieved. There is a need to evaluate cloud systems to ensure that the desired benefits from these systems are being achieved. However, organizations often find themselves unable to assess the full implications of their IS infrastructure or let alone their cloud architecture for that matter. This is because the intangible and non-financial benefits, which are hard to value, complicate the process (Irani, 2002). Cronholm and Goldkuhl (2003) claimed that evaluating IT-systems is never an easy task.

The IS literature on evaluations is separated into the following two camps: qualitative evaluation techniques and quantitative evaluation techniques. Qualitative approaches to evaluating information systems are concerned with softer user-oriented criteria such as use, user satisfaction, individual impact, system quality, information quality, and organizational impact which can be use to evaluate systems success (DeLone and McLean, 1992). However, the more prevalent evaluation approach espoused in the IS literature is the more formal and structured quantitative approach,
which focuses on a cost benefit analysis based on a defined set of criteria (Irani, 2002; Dhillon, 1995; Walsham, 2006).

A challenge in the cloud privacy evaluation process is that many of the traditional IS evaluation techniques are a simple check the box type of evaluation. Checklists are very often derived directly from audit frameworks or methodologies as a simplified tool to show the degree of conformity to a specified standard. A problem with this checklist approach is that every organization should have its own unique privacy strategy, which is dependent on their organization’s strategic visions, that drives their cloud privacy policies and practices. Therefore applying a cookie cutter approach to evaluating cloud privacy practices will only ensure that the basic minimal privacy requirements are being met and will not guarantee that the privacy strategy goals are being met. With respect to evaluation of information security systems Dhillon (1995) argued that organizations’ need to develop evaluation procedures that complement their strategic security vision. Essentially this view towards evaluation purports that the purpose of any evaluation process within an organization is to ensure its strategic goals are incorporated into the process being evaluated.

6.3.1 Synthesized Perspective of the Evaluation Process

It is important that organizations operating in cloud environment evaluate their information handling practices and systems for possibilities of exposure to information privacy risks. The following section discusses an evaluation approach that utilizes a formal evaluation approach to develop a holistic approach to evaluating cloud privacy
practices. A holistic evaluation approach is one that is based on the internal needs of an organization and provides management with an understanding the added value and costs that result from their privacy related activities. This means that the first objective of a cloud privacy evaluation is not to ensure the highest level of privacy is being provided but rather to determine if the level of privacy being provided is not too restrictive to the business needs and helps them achieve operational goals. The evaluation of cloud privacy is a tool for management to administer cloud privacy, to determine whether cloud privacy objectives have been met and thus determine whether privacy risk objectives have also been satisfied. Cloud privacy evaluations will help management to govern privacy risks in cloud computing environments.

A multidimensional evaluation approach for evaluating cloud privacy will provide management with a broad perspective of their cloud privacy practices. Barnard and Solms (2000) developed a multidimensional evaluation approach evaluating security controls in IT environments. Because of the broad nature of this evaluation approach it is appropriate for evaluating privacy in cloud computing environments. The four dimensions incorporated into this evaluation approach are functionality, assurance of correctness, assurance of effectiveness, and assurance of operation (Barnard and Solms, 2000). Each of these dimensions needs to be evaluated individually based on criteria established by an organizations cloud privacy strategy to effectively evaluate cloud privacy. Functionality refers to the aspect that all the proposed privacy controls are in fact present in the cloud environment being evaluated. After ensuring that the cloud privacy controls are established the next step in the evaluation process is assurance of
correctness, which ensures they are correctly installed and operational. During this evaluation step each and every control should be tested to determine if it is has been implemented correctly. Assurance of effectiveness is the third step of this evaluation process. Evaluating for effectiveness will assess the ability of the proposed and installed cloud privacy controls to achieve the level of privacy protection espoused in the cloud privacy strategy. Assurance of operation is the final step in this evaluation approach. Assurance of operation refers to the evaluation of all the operational procedures that support the cloud privacy controls to ensure requisite personnel are following them. It is important to note that this evaluation process is more comprehensive than most checklists where only functionality is evaluated. This evaluation approach effectively and comprehensively ensures that cloud privacy objectives are met.

6.4 Auditing Cloud Privacy Practices

The advantages of cloud computing such as the ability to easily scale to meet growing technology needs, increase data storage capacity, and share services in a dynamic environment also increase the risk to the protection of information privacy. Risks has been described as a negative outcome that has a known or estimated probability of occurrence based on experience or some theory (Loudon and Loudon, 1991). Privacy is a key business risk and compliance issue, because it resides at the center of social norms, human rights and legal requirement (Ackerman et al. 2001). Privacy risk refers to exposure to such consequences as: failure to protect information privacy; unauthorized disclosure of personal information, inappropriate use of personal information, failure to comply with privacy regulations. Organizations
operating in the cloud can demonstrate control over the life cycle of personal information, i.e. from collection to destruction, by conducting cloud privacy audits to ensure that they are complying with their stated privacy policies and required privacy regulations.

The primary reason of having any audit is to limit an organization’s exposure to risk. Because of the increased legal complexity in cloud computing environments, Pearson and Charlesworth (2009) suggests that companies conduct cloud privacy audits to protect themselves and their customers from legal liabilities. A challenge in performing a cloud privacy audit is that there is no existing privacy audit framework developed specifically for cloud computing environments. An audit is a systematic process of obtaining and evaluating evidence regarding assertions about economic actions and events in order to determine how well they correspond with established criteria (Romney, 2009). The majority of the IS audit frameworks being used today focus on the audit process from a financial perspective. The industry standard is to design a privacy audit around the AICPA’s generally accepted privacy principles (GAPP). These principles provide very limited guidance as to what needs to be included in a privacy audit program. For example the first principle denoted as the management principle states, “the entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.” An audit step for this could simply be that the auditor verifies that a position job description includes the responsibility for ensuring a privacy policy exists. As long as this job description was communicated to the employee who maintains that position then this would satisfy the
audit requirement of this step. Although this a simplistic view of applying GAPP it would satisfy the requirements of a privacy audit. However, an audit in this form misses the purpose of having an audit performed, which is to first ensure legal compliance, second ensure compliance with external contractual agreements, thirdly, ensure compliance with internal control standards, and lastly to improve the organizations privacy practices over time.

An audit of cloud privacy policies and practices ensures that organizations utilizing cloud technologies are meeting the internal and external privacy requirements. Internal privacy requirements are driven by organizational privacy goals and policies. External privacy requirements are typically stipulated by either privacy regulations, which can vary depending on the legal jurisdiction, or by contractual agreements with clients. A cloud privacy audit should focus on collecting and evaluating evidence to determine if an organization is managing their cloud privacy practices such that they meet established privacy criteria. We propose that a cloud privacy audit could benefit from using the cloud privacy audit framework (CPAF) developed in our research as criteria to audit cloud privacy. For example with CPAF as audit criteria we could create additional audit steps surrounding the effectiveness of privacy management; such as verifying that management evaluates governance of the privacy policy periodically, or that management review internal controls effecting information privacy at least once a year. These are just a few examples as to how the CPAF could improve the privacy audit functions and help to ensure information privacy in cloud computing.
6.5 Conclusion

The purpose of this chapter was to provide a synthesis of this research studies implications for managing information privacy in cloud computing. A key aspect of this discussion is how to manage the privacy risks associated with cloud computing. There needs to a focus by management to proactively manage their privacy practices and policies such that they are able to minimize privacy risks while maintaining the highest economic benefit to the company as possible. There are no definitive management methods or techniques to eliminate all privacy risks and still achieve all of the corporate strategic goals. We discussed the importance of management be able to formulation a cloud privacy strategy that is aligned with their corporate strategic goals. This strategic planning process can be improved by incorporating Segars and Grover (1999) dimensions strategic planning process and the cloud privacy audit objectives from our study. Secondly we recommend that organizations develop a multidimensional evaluation approach for evaluating their cloud privacy practices. We recommend utilizing Barnard and Solms (2000) approach to evaluating systems which include incorporating the following four aspects into the evaluation approach: functionality, assurance of correctness, assurance of effectiveness, and assurance of operation. Lastly we espoused the importance of conducting a cloud privacy audit on a regular basis to reduce cloud privacy risk. Also we recommend incorporating the CPAF from this study as privacy audit criteria because it is important to utilize a more detail privacy perspective within existing audit practices to ensure all stakeholders privacy objectives are being met. Additionally, performing cloud privacy audits on a regular basis verifies
that privacy policies and regulations are being followed, and provides a level of comfort
to cloud users that the privacy of his or her personal data is being protected. In order to
achieve the desired competitive advantages from the adoption of cloud technologies
organization’s management teams needs to be able to successfully apply these skills into
their privacy management process.
Chapter 7 Summary

7.1 Introduction

This thesis argues that information privacy is at risk due to the rapid advancements in cloud computing technology and the lack of a privacy framework to protect personal information in the cloud. With the increased value of information and amount of information being processed in the cloud, organizations are tempted to impede their customer’s privacy. It is too easy for organizations to look the other way when individuals’ privacy is being infringed upon when privacy expectations are not clearly defined. It is argued that there is a lack of an understanding as to what organizations need to do in order to protect individuals’ privacy. Culnan and Williams (2009) called for privacy researchers to study; how organizations should handle personal identifiable information, what are organizations responsibilities towards information privacy protection, and the moral duties organizations have to protect their customers and stakeholders’ privacy needs. The motivation for this research is based on the established understanding in the privacy literature that technology advancements result in a loss of privacy.

According to a recent Gartner Research report (Marston et al., 2011) cloud computing is positioned to be $150 billion business by 2014, and according to AMI partners, small and medium businesses are expected to invest over $100 billion in cloud technology by 2014. The reason for this rapid expansion of cloud computing is the promise of a more efficient and powerful technology platform at a fraction of the cost of traditional technology infrastructures. However, unresolved privacy issues impose strong barriers to adoption of cloud technologies (Zhou et al., 2010). These
privacy issues undermine individuals’ confidence towards entrusting sensitive information to cloud computing service providers. The concern for information privacy, in the cloud, is significant enough that companies utilizing cloud platforms and services need to ensure public trust. Organizations need to develop privacy policies and privacy management practices that are socially responsible towards their customers’ privacy.

One way to build public trust is by having an independent audit performed to provide evidence that an organization is adhering to their stated policies and regulatory requirements. Our review of information systems and accounting information systems literature found limited recourses that support the notion of existing privacy audit frameworks for cloud computing. Ko et al. (2011) argued that additional research is needed to help increase the accountability and auditability of cloud service providers. This thesis answers this call by developing a cloud privacy audit framework. This framework can be used, as a management tool, to reduce privacy risks and strengthen controls around information handling practices.

The purpose of this chapter is to provide a final synthesis of this study’s research findings and to identify the contributions of this thesis. The remainder of this chapter will provide a summary of the research performed in this two phase study, followed by a discussion on this research study’s contributions, limitations and future research goals.

7.2 Summary of Research Performed

7.2.1 Value Focus Thinking Phase of Study

This dissertation was conducted as a two-phase study whereby the first phase seeks to understand an individual’s privacy values and their cloud privacy objectives. In the first phase, Keeney’s (1992) value focus thinking approach is utilized to
identify individual privacy values with respect to emerging cloud technologies and to
develop an understanding of cloud privacy objectives. During this phase, we
interviewed 90 individuals to identify values of individuals with regards to their privacy
values in the context of cloud computing. We then applied data analysis techniques, as
recommended by Keeney (1994) and Dhillon and Torkzadeh (2006), to identify cloud
privacy objectives. This first phase resulted in the identification of six fundamental
objectives and nineteen means objectives with respect to cloud privacy.

7.2.2 Design Science Phase of Study

The second phase uses a design science research approach for the development
and design of a cloud privacy audit framework. For this phase, we adopted Peffers et al.
(2008) design science research methodology (DSRM), which provide a rigorous
framework for conduct design science research. DSRM incorporates an iterative process
that includes the following steps: problem identification and motivation, definition of the
objectives for a solution, design and development, demonstration, evaluation, and
communication. During this phase, we utilized the results from phase one to establish
the cloud privacy audit objectives from which to begin the design the cloud privacy
audit framework. During this phase of the study, we utilized focus groups during the
design and evaluation process as recommended by Tremblay et al. (2010). We used an
exploratory focus group of industry experts to develop and design of the cloud privacy
audit framework. For the evaluation process, we utilized a confirmatory focus group of
information system security auditors to evaluate the cloud privacy audit framework. This
phase of the study resulted in a cloud privacy mean and fundamental relationship matrix
and a cloud privacy audit framework. The matrix is based on the
understanding that was developed through in depth discussions with the exploratory focus group about how they interpret the cloud privacy objectives to be interlinked. The cloud privacy audit framework is grounded in the identified cloud privacy objectives from phase one. The framework provides management a tool to assist them in the strategic development of privacy policies and privacy management practices such as resource allocations for the protection of information privacy, privacy impact analysis for new cloud computing solutions being considered, privacy risk assessments during operational and financial audits.

7.3 Contributions of this thesis

In order to be considered “good research”, a design science research study ought to provide a solution to an unsolved problem in a unique and innovative way or at least provide a more streamlined approach to a problem (Hevner et al., 2004). Peffers et al. (2008) considered the communication of the effectiveness of the design artifact to researchers and practitioners and important component of the research process so much that he included it as the final step in his design science research methodology approach. Given these perspectives towards the value of good research being able to contribute to a body of knowledge, elevates the importance of articulating the contributions of a dissertation. Several unique and innovation contributions have emerged from this dissertation study that add to the existing body of knowledge. These contributions are discussed in the following three subsections: theoretical contribution, methodological contribution, and practical contribution.
7.3.1 Theoretical Contribution

Privacy is a complex and multi-dimensional concept, which makes it difficult to define. Researchers from many disciplines such as law, sociology, psychology, management, and information systems have debated the concept of privacy. Each discipline has typically adopted its own view towards privacy. These perspectives have ranged from a process view, psychological view, to a behavioral view (Margulis, 2003). A process perspective towards privacy is the belief that individuals regulate social interactions thereby selectively controlling access to one’s self (Altman, 1977). A psychological perspective emphasizes privacy as a control over unwanted access (Allen, 1988; Margulis, 1977). A behavioral perspective of privacy stresses control over transactions that regulate access to self, such that it reduces vulnerability and increases decisional and behavioral options (Margulis, 2003). For the purpose of this dissertation it is important to understand theoretical stance of these various perspectives because they are the theoretical foundations used by information systems researchers to study information privacy.

This dissertation has two main theoretical contributions. First it is important to reiterate that, for this dissertation research, we adopted an abductive research strategy as defined by Blaikie (2007). The aim of this research approach is to describe and understand social life in terms of social actors’ motives and understanding. In order to start this process, the researcher discovers every day lay concepts, meanings and motives. From this, the researcher produces a technical account from lay accounts. The research then uses this new understanding to develop a theory and test it iteratively. Given this stance towards this dissertation research, one of the main contributions is the
creation of a theoretical framework for protecting information privacy in the context of cloud computing. The Cloud Privacy Audit Framework developed in this dissertation provides a foundation for future researchers to understand and the complexities surrounding the concept of information privacy in cloud computing. A second theoretical contribution made by this dissertation study is the cloud privacy relationship model. The privacy objective relationship matrix model, developed in this study through an in depth analysis with the exploratory focus group, provides a stepping stone for future researchers to develop additional privacy models to measure the significance of various privacy controls and their effectiveness in ensuring information privacy.

7.3.2 Methodology Contribution

The methodological contribution involves the unique application of Value Focus Thinking within the context of performing a design science study. The design science paradigm has long been established in the in fields of engineering and sciences (Simon, 1996); however, it has only recently gained acceptance in the domain of information systems research as a legitimate form of research (Hevner, 2007; Peffers et al., 2008). Peffers et al. (2008) formally defined a research methodology for use in IS, called a Design Science Research Methodology (DSRM). The process includes six steps or stages: problem identification and motivation, definition of the objectives for a solution, design and development, demonstration, evaluation, and communication. Peffers et al (2008) argued that since the DSRM approach is an iterative process that the impetus of the design science study could start in any of the first four stages. The unique methodological contribution of this thesis is the utilization of Keeney’s (1992) Value Focused Thinking approach to define the objectives to be utilized in the
design study. The use of this value-based approach to start the development of a design artifact ensures that the relevance of the resulting artifact.

7.3.3 Practical Contribution

One practical contribution of this dissertation reside in the ability of IS auditors to develop an audit plan that provides assurance of key privacy risks and concerns such that it reduces the audit risk of failing to identify a missing control or control weakness in an organization’s privacy policy and practices. By better understanding individuals’ privacy expectations and objectives within in the complex environment of cloud computing, IS auditors may be best able to create and execute a privacy audit which provides optimal coverage for ensuring information privacy practices have been effectively implemented within an organization utilizing cloud technologies. One objective espoused by the Cloud Privacy Audit Framework that auditors may want to focus on is the fundamental privacy objective to increase trust with the cloud provider. Based on our discussion with the IS audit team, auditors have historically maintained the belief that if they have a clean audit, the readers of the audit report should be able to trust the organization that was audited. However, this may or not have been the case, depending on the audit knowledge of the user of the audit report. By designing the cloud privacy audit program to include items from the CPAF under the area of increasing trust with the cloud provider such as testing controls around secure data transfers, evaluating internal control policies, verifying the processes around privacy risk assessments, and determining if privacy policies and practices are effectively communicated, auditors can ensure that they have address specific areas of individual’s cloud privacy concerns which would help to improve trust in the cloud providers privacy practices.
This planning process can be repeated, for each of the fundamental objectives, to ensure the scope of the audit program provides optimal coverage of individuals’ privacy concerns for cloud computing.

A second practical contribution that has emerged from this dissertation is that IS practitioners could use the CPAF to be able to help formulate a strategy to protect information privacy when implementing a cloud technology solution. When designing privacy practices for cloud applications or services an organization could reference the CPAF as a tool to ensure that have addressed the primary privacy concerns individuals have with respect to cloud computing. For example, a cloud service provider could establish the practice of writing customized service contracts with each customer to ensure that all their privacy requirements are met. A cloud service provider could also implement a strategy where they design cloud-computing environments and privacy controls based specific industry privacy regulation requirements. Both of these privacy practices would support sub-objectives of the fundamental cloud privacy objective to maximize protection of rights to privacy. One would help ensure service contract meet privacy requirement the other would help limit liability concerns due to privacy regulations. These are the more notable practical contributions have emerged from this thesis.

7.4 Limitations

There are two major limitations to the first phase of this research study; one is generalizability of the cloud privacy objectives, and the second is research bias. The first limitation towards the generalizability of this study is found in the issue that the non-random selection of master level students to represent the general population
of cloud users. This is because the level of knowledge of master students with respect to technology usage and privacy threats maybe higher than an average person. This increased knowledge base could likely result in the students having a higher level of privacy awareness. This view is supported by the findings of Weisband and Reining’s (1995) study of education and training affects on privacy awareness. Since this study is focused on cloud privacy, we felt that the research participants' increased knowledge of technology usage, including that of cloud technology, was a benefit that outweighed risks associated with not having a random selection of the general population.

The second limitation in the first phase of this study is concerned with researcher bias. A common criticism of qualitative research is that risk of researcher bias during the interpretive process. For the purpose of addressing concerns of researcher bias, it is important to understand our position for conducting this research. The nature of the first research question was to understand individuals values with respect to information privacy in cloud computing. The newness and unique qualities of privacy issues in cloud computing are better fitted to a qualitative study where issues can emerge naturally through a holistic approach apposed to trying to force fit an existing set of variables or constructs into the context of privacy and cloud computing. With the abductive research strategy approach adopted in this study, the researcher needs to understand about the research subjects’ reality, and how it is constructed through the knowledge individuals’ use in the production, reproductions and interpretation of the phenomenon under investigation (Blaikie, 2007). It is then the responsibility of the research to transcribe abstract individual motives and actions into different types of motives for different types of actions for a particular situation. From this transcription, a researcher can
then classify the motives and actions to provide an understanding of the social activities and may lead to a more systematic explanatory account of the phenomenon being studied (Blaikie, 2007). In order to minimized researcher bias in the interpretive process of converting raw values from the transcribed data into the common form objectives as Keeney (1994) recommended we incorporated a check and balance procedure into the process. First, I as the researcher initially converted a sample of the raw values into common form objectives. Secondly, my advisor who has expertise in applying the Value Focus Thinking approach evaluated the results to ensure the common form objectives were a fair representation of the initial raw values. This check and balance process was reiterated until my advisor felt I had the adequate skills to continue on my own.

The limitations of the second phase of this research study lie in the limited number of people who participated in the evaluation. Three issues limit the scale of evaluation in this study. For starters, the target participants need to be familiar with IS auditing concepts and practices for cloud computing. Secondly, the cloud privacy audit framework needs to be explained in detail and participants need to have a fairly good understanding of it. Lastly, to test the effectiveness of the CPAF it needs to be utilized, in the field, to develop a cloud privacy audit program and then evaluated based on the implementation of the audit program. Thus, to compensate for these issues we utilized a Confirmatory Focus Group with expertise in IS security audits were the CPAF was evaluated through an iterative process until the group members were satisfied their ability to implement the CPAF into their audit planning process. Since the CFG discussions were the principal evaluation methods, qualitative data was collected as the major type of evaluation data to be analyzed. This data was analyzed utilizing
the theory of Technology Acceptance Model as a theoretical lens to evaluate the CFG members’ perceived usefulness and perceived ease of use of the CPAF. Although qualitative data analysis shows a positive and satisfying evaluation result, it is difficult to generalize such a result and make a resounding conclusion for a broad context. Lastly, the evaluation in this phase of the research only tested CFG members’ perceptions of CPAF utility by their self-reported feelings and experiences. The objectivity of user comments may be questioned. It would be better if direct application of the CPAF during an audit planning process and its direct impact could be measured.

7.5 Future Research Directions

The purpose of this section is to draw out implications for future research related to the protection of information privacy and the adoption of the CPAF. For starters, the next logical step should attempt to minimize some of the limitations identified in this study. The first would be to test the cloud privacy objective relationship model through the use of quantitative data. Developing a survey based on the 105 sub-objects identified in phase one of this study, and then performing a confirmatory factor analysis on the collected quantitative data could be one way to test the means and fundamental objectives relationship model.

A second research study could be designed as an action research study where an organization that needs to have a privacy audit performed utilizes the CPAF to design and implement a cloud privacy audit. These of such a study would also help to extend the CPAF to include actual audit steps that are design to test and support the objectives of the CPAF.
A third study could be designed to link the findings from the confirmatory factor analysis to create a privacy objective model and tested through the use of structural equation modeling techniques. This would allow for statistical testing for each of the paths between the means and fundamental objectives relationship model.

A fourth study could develop a decision model for prioritizing information privacy risks. Such a model could assist management in the resource allocation process when resources are limited. This could be accomplished through a research study that incorporates the use of objective decision analysis techniques.

Lastly, future research resulting from this dissertation could focus on the application of Value Focus Thinking within the Design Science Research Methodology. This study showed that utilizing value focus thinking within the scope of DSRM could strongly improve the rigorous process of developing relative and insightful objectives for design science studies.
Appendix A Interview Questions

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Are you familiar with the term cloud computing?</td>
</tr>
<tr>
<td>2</td>
<td>What does the concept of privacy mean to you?</td>
</tr>
<tr>
<td>3</td>
<td>Are there certain types of information or data that you treat different from other data?</td>
</tr>
<tr>
<td>4</td>
<td>Interview questions for Understanding Individual Privacy Objectives for Cloud Environment study.</td>
</tr>
<tr>
<td>5</td>
<td>Consider your own belief system and values that lead you to behave the way you do with respect to your own data and information.</td>
</tr>
<tr>
<td>6</td>
<td>How private are you with your personal information?</td>
</tr>
<tr>
<td>7</td>
<td>Do you have the same privacy view towards work files or information required for your job?</td>
</tr>
<tr>
<td>8</td>
<td>How do you currently interact with information in the cloud? (i.e. personal, work, school)</td>
</tr>
<tr>
<td>9</td>
<td>What type of information are you willing to have used in the cloud?</td>
</tr>
<tr>
<td>10</td>
<td>What type of information do you not want in the cloud?</td>
</tr>
<tr>
<td>11</td>
<td>Do you have any concerns regarding the protection of your personal information?</td>
</tr>
<tr>
<td>12</td>
<td>Have you always had this view towards privacy or has it changed over time? If so how has it changed?</td>
</tr>
<tr>
<td>13</td>
<td>Are you concerned about your personal information being available in the cloud?</td>
</tr>
<tr>
<td>14</td>
<td>How do you manage what information you make available in the cloud?</td>
</tr>
</tbody>
</table>
Appendix B List of Sub-Objectives for cloud Privacy

<table>
<thead>
<tr>
<th></th>
<th>Sub-Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Ensure future access to my information by selecting a service provider who has a stable future.</td>
</tr>
<tr>
<td>2</td>
<td>Ensure that my cloud service provider uses encryption tools to protect my information.</td>
</tr>
<tr>
<td>3</td>
<td>Ensure that the cloud service provider has similar privacy values that I have.</td>
</tr>
<tr>
<td>4</td>
<td>Identify a cloud service provider who has a stable future.</td>
</tr>
<tr>
<td>5</td>
<td>Limit the amount of information I disclose on social media websites.</td>
</tr>
<tr>
<td>6</td>
<td>Limit the amount of personal information I provide to organizations using cloud services.</td>
</tr>
<tr>
<td>7</td>
<td>Limit the amount of personal information in the cloud.</td>
</tr>
<tr>
<td>8</td>
<td>Limit the disclosure of information that can personally identify me.</td>
</tr>
<tr>
<td>9</td>
<td>Limit the disclosure of religious affiliations and political views.</td>
</tr>
<tr>
<td>10</td>
<td>Segregate information about myself into specific identity groupings such as personal, family, friends, professional, and academic.</td>
</tr>
<tr>
<td>11</td>
<td>To ensure the cloud service provider has a strict hiring process of employee.</td>
</tr>
<tr>
<td>12</td>
<td>To minimize the disclosure of personal information.</td>
</tr>
<tr>
<td>13</td>
<td>To audit the cloud service provider to ensure they are following their privacy policy.</td>
</tr>
<tr>
<td>14</td>
<td>To audit the cloud service provider to ensure they are following their privacy regulations.</td>
</tr>
<tr>
<td>15</td>
<td>To be informed about the privacy status of my personal information.</td>
</tr>
<tr>
<td>16</td>
<td>To be properly notified when there is a privacy/security breaches.</td>
</tr>
<tr>
<td>17</td>
<td>To clearly define who owns the data stored in the cloud.</td>
</tr>
<tr>
<td>18</td>
<td>To ensure access to personal information at a future date through reliable data backups.</td>
</tr>
<tr>
<td>19</td>
<td>To ensure I am current with technology advancements.</td>
</tr>
<tr>
<td>20</td>
<td>To ensure internal controls are established to protect my information.</td>
</tr>
<tr>
<td>21</td>
<td>To ensure privacy regulations stay current with the capabilities of emerging technologies.</td>
</tr>
<tr>
<td>22</td>
<td>To ensure protection of personal information in the cloud through regulation and industry design standards.</td>
</tr>
<tr>
<td>23</td>
<td>To ensure technical security measures are being used to protect my personal information.</td>
</tr>
<tr>
<td>24</td>
<td>To ensure that cloud service providers consider being data custodians as an important aspect of their service.</td>
</tr>
<tr>
<td></td>
<td>To ensure that I have the ability to change service providers when I choose to do so.</td>
</tr>
<tr>
<td>---</td>
<td>--------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>26</td>
<td>To ensure that I know whom I am giving my personal information to.</td>
</tr>
<tr>
<td>27</td>
<td>To ensure that my anonymity is protected.</td>
</tr>
<tr>
<td>28</td>
<td>To ensure that my cloud service provider does not share my information with a third party.</td>
</tr>
<tr>
<td>29</td>
<td>To ensure that my cloud service provider respects my rights for privacy</td>
</tr>
<tr>
<td>30</td>
<td>To ensure that my data is removed from the cloud server when I terminate my service agreement</td>
</tr>
<tr>
<td>31</td>
<td>To ensure that my passwords are well protected and secure</td>
</tr>
<tr>
<td>32</td>
<td>To ensure that my personal information is compartmentalized within the server based on who needs to view the information</td>
</tr>
<tr>
<td>33</td>
<td>To ensure that my personal information is stored in a safe jurisdiction</td>
</tr>
<tr>
<td>34</td>
<td>To ensure that only people I authorize have access to my personal information.</td>
</tr>
<tr>
<td>35</td>
<td>To ensure that the cloud service provider follows local privacy laws.</td>
</tr>
<tr>
<td>36</td>
<td>To ensure that the cloud service provider has a proper security/privacy training program for their employees.</td>
</tr>
<tr>
<td>37</td>
<td>To ensure that the cloud service provider has high ethical standards</td>
</tr>
<tr>
<td>38</td>
<td>To ensure that the latest technology and software are utilized to protect my information</td>
</tr>
<tr>
<td>39</td>
<td>To ensure the accessibility to my personal information in the cloud.</td>
</tr>
<tr>
<td>40</td>
<td>To ensure the authentication process is efficient and secure.</td>
</tr>
<tr>
<td>41</td>
<td>To ensure the cloud service provider has good monitoring practices of their infrastructure.</td>
</tr>
<tr>
<td>42</td>
<td>To ensure the physical security of the technology infrastructure housing my personal information</td>
</tr>
<tr>
<td>43</td>
<td>To ensure the protection of personal information through third party validation.</td>
</tr>
<tr>
<td>44</td>
<td>To ensure the security of personal information</td>
</tr>
<tr>
<td>45</td>
<td>To ensure the security of personal information in the cloud</td>
</tr>
<tr>
<td>46</td>
<td>To find a cloud service provider who I can trust with my personal information</td>
</tr>
<tr>
<td>47</td>
<td>To have standard international privacy laws for the cloud.</td>
</tr>
<tr>
<td>48</td>
<td>To hold cloud service providers legal liable for privacy/security breaches</td>
</tr>
<tr>
<td>49</td>
<td>To identify cloud service providers who have not had any legal issues</td>
</tr>
<tr>
<td>50</td>
<td>To identify a stable company I can trust with my personal information.</td>
</tr>
<tr>
<td>51</td>
<td>To increase the methods available to gain access to information stored in the cloud.</td>
</tr>
<tr>
<td>52</td>
<td>To increase understanding of the cloud's security infrastructure</td>
</tr>
<tr>
<td>53</td>
<td>To increase user responsibility towards protecting their own information.</td>
</tr>
<tr>
<td></td>
<td>Reason</td>
</tr>
<tr>
<td>---</td>
<td>-------------------------</td>
</tr>
<tr>
<td>54</td>
<td>To know where my personal information is being stored</td>
</tr>
<tr>
<td>55</td>
<td>To limit my cloud service provider's access to my information to those who absolutely need access.</td>
</tr>
<tr>
<td>56</td>
<td>To limit the collection of my information collected by my cloud service provider or third party</td>
</tr>
<tr>
<td>57</td>
<td>To limit the control governments have over access to my personal information</td>
</tr>
<tr>
<td>58</td>
<td>To limit third parties from accessing my personal information</td>
</tr>
<tr>
<td>59</td>
<td>To maintain intellectual property rights to my information</td>
</tr>
<tr>
<td>60</td>
<td>To manage disclosure of personal information</td>
</tr>
<tr>
<td>61</td>
<td>To maximize control of my identity</td>
</tr>
<tr>
<td>62</td>
<td>To maximize control over my personal information</td>
</tr>
<tr>
<td>63</td>
<td>To maximize control over who can access my personal information</td>
</tr>
<tr>
<td>64</td>
<td>To maximize efficiencies for data transfers between systems.</td>
</tr>
<tr>
<td>65</td>
<td>To maximize the availability of information when needed</td>
</tr>
<tr>
<td>66</td>
<td>To maximize the availability of the cloud services</td>
</tr>
<tr>
<td>67</td>
<td>To maximize the availability of the internet connection to my information.</td>
</tr>
<tr>
<td>68</td>
<td>To maximize the convenience of accessing my information in the cloud</td>
</tr>
<tr>
<td>69</td>
<td>To maximize the cost benefit of using the cloud</td>
</tr>
<tr>
<td>70</td>
<td>To maximize the ease of use with respect to cloud technology</td>
</tr>
<tr>
<td>71</td>
<td>To maximize the efficiency of increasing the capacity of the system.</td>
</tr>
<tr>
<td>72</td>
<td>To maximize the protection of my personal identity</td>
</tr>
<tr>
<td>73</td>
<td>To maximize the reliability of cloud services</td>
</tr>
<tr>
<td>74</td>
<td>To maximize the security of the cloud's IT infrastructure</td>
</tr>
<tr>
<td>75</td>
<td>To maximize the understanding the risk involved with using a cloud service provider</td>
</tr>
<tr>
<td>76</td>
<td>To maximize time efficiency with respect to data transfers</td>
</tr>
<tr>
<td>77</td>
<td>To minimize changes to privacy policy agreements</td>
</tr>
<tr>
<td>78</td>
<td>To minimize misunderstandings with respect to cloud provider's privacy policy</td>
</tr>
<tr>
<td>79</td>
<td>To minimize privacy/security risks while maximize benefits of cloud services</td>
</tr>
<tr>
<td>80</td>
<td>To minimize risk of using the cloud services</td>
</tr>
<tr>
<td>81</td>
<td>To minimize the amount of personal information provided to cloud providers I do not trust.</td>
</tr>
<tr>
<td>82</td>
<td>To minimize the challenges of using cloud technologies</td>
</tr>
<tr>
<td>83</td>
<td>To minimize the possibility of privacy or security breaches.</td>
</tr>
<tr>
<td>84</td>
<td>To minimize the risk of having my personal data corrupted</td>
</tr>
<tr>
<td>85</td>
<td>To monitor my profile accounts to ensure access to my personal information is granted only to those I authorize to have it</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>--------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>86</td>
<td>To only disclose information for legitimate reasons</td>
</tr>
<tr>
<td>87</td>
<td>To perform a risk assessment of privacy breaches before using the cloud</td>
</tr>
<tr>
<td>88</td>
<td>To perform a risk assessment of using the cloud service</td>
</tr>
<tr>
<td>89</td>
<td>To protect my financial information</td>
</tr>
<tr>
<td>90</td>
<td>To protect my information from hackers</td>
</tr>
<tr>
<td>91</td>
<td>To protect my information through well defined internal controls and procedures.</td>
</tr>
<tr>
<td>92</td>
<td>To protect my medical information</td>
</tr>
<tr>
<td>93</td>
<td>To protect my privacy rights with a legal contract</td>
</tr>
<tr>
<td>94</td>
<td>To protect my reputation</td>
</tr>
<tr>
<td>95</td>
<td>To protect personal information stored on a server</td>
</tr>
<tr>
<td>96</td>
<td>To protect the integrity of my personal data</td>
</tr>
<tr>
<td>97</td>
<td>To protect the privacy of my personal information</td>
</tr>
<tr>
<td>98</td>
<td>To provide a secure environment for collaboration with others</td>
</tr>
<tr>
<td>99</td>
<td>To reduce my legal responsibility/risk.</td>
</tr>
<tr>
<td>100</td>
<td>To reduce the governments ability to cease my information</td>
</tr>
<tr>
<td>101</td>
<td>To reduce the like likelihood of hackers gaining access to my information</td>
</tr>
<tr>
<td>102</td>
<td>To reduce the risk of privacy breaches.</td>
</tr>
<tr>
<td>103</td>
<td>To use a reputable cloud service provider</td>
</tr>
<tr>
<td>104</td>
<td>To utilize a cloud service provider with a positive reputation</td>
</tr>
<tr>
<td>105</td>
<td>To utilize encryption to protect my information while the data is in transit</td>
</tr>
</tbody>
</table>
References


Awad, N.F., Krishnan, M.S., (2006), The personalization privacy paradox: an empirical evaluation transparency and the willingness to be profiled online for personalization”, MIS Quarterly, Vol. 30 Iss. 1


Chen, Z., & Yoon, J. (2010). IT auditing to assure a secure cloud computing. In 6th World Congress on Services (pp. 253-259).


198


Kitzinger J. (1994) ‘The methodology of focus groups: the importance of interaction between research participants’, Sociology of Health 16 (1): 103-21.


Lee, A. (2000, May). Systems thinking, design science, and paradigms: heeding three lessons from the past to resolve three dilemmas in the present to direct a trajectory for future research in the information systems field. Keynote Address. In Eleventh International Conference on Information Management, Taiwan.


McDonald, K. T. (2010). *Above the clouds: Managing risk in the world of cloud computing.* IT Governance Ltd.


European Data Protection: In Good Health? (pp. 251-265). Springer Netherlands.


Tremblay, M. C., Hevner, A. R., & Berndt, D. J. (2010). The use of focus groups in design science research. In Design Research in Information Systems (pp. 121-143). Springer US.


Chicago
