Cloud privacy objectives a value based approach

David Lewis Coss
Department of Accounting and Legal Studies, School of Business and Economics,
College of Charleston, Charleston, South Carolina, USA, and

Gurpreet Dhillon
Department of Information and Supply Chain Management,
Bryan School of Business and Economics,
University of North Carolina at Greensboro, Greensboro, North Carolina, USA

Abstract

Purpose – To effectively develop privacy policies and practices for cloud computing, organizations need to define a set of guiding privacy objectives that can be applied across their organization. It is argued that it is important to understand individuals’ privacy values with respect to cloud computing to define cloud privacy objectives.

Design/methodology/approach – For the purpose of this study, the authors adopted Keeney’s (1994) value-focused thinking approach to identify privacy objectives with respect to cloud computing.

Findings – The results of this study identified the following six fundamental cloud privacy objectives: to increase trust with cloud provider, to maximize identity management controls, to maximize responsibility of information stewardship, to maximize individual’s understanding of cloud service functionality, to maximize protection of rights to privacy, and to maintain the integrity of data.

Research limitations/implications – One limitation is generalizability of the cloud privacy objectives, and the second is research bias. As this study focused on cloud privacy, the authors 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 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 opposed to trying to force fit an existing set of variables or constructs into the context of privacy and cloud computing.

Practical implications – The findings of this research study can be used to assist management in the process of formulating a cloud privacy policy, develop cloud privacy evaluation criteria as well as assist auditors in developing their privacy audit work plans.

Originality/value – Currently, there is little to no guidance in the literature or in practice as to what organizations need to do to ensure they protect their stakeholders privacy in a cloud computing environment. This study works at closing this knowledge gap by identifying cloud privacy objectives.

Keywords Privacy, Cloud computing, Value focus thinking

Paper type Research paper

Information privacy is an increasing concern for business leaders today. According to Identity Theft Resource Center during 2016 the number of data breaches increased to 1093 a 40 per cent increase from the year before (Identity Theft Resource Center, 2017). Just four of these breaches resulted in 120 million social security numbers being released. That is about 1 in 3 Americans who have had the personal information exposed in just one year. Even with widespread data breaches such as these individuals are still eagerly adopting new technologies to meet their informational and social needs. Along with the rapid evolution of information technologies the value of information has increased, resulting in organizations
demanding the utilization of more data than ever before. Many organizations are finding it difficult to meet these demands because resources are limited. With recent advancement in technologies and the lower cost of connectivity, cloud computing is becoming a viable solution for them. Cloud computing uses a network of remote servers hosted on the internet to store, manage and process data. While on one hand cloud computing is good for managing the cost of IT, on the other hand, there is a concern about organizations ability to ensure information privacy across multiple technology platforms and jurisdictional boundaries (Dinev et al., 2009; Dhillon and Kolkowska, 2011).

These privacy concerns are also compounded in cloud computing environments due to the pervasive nature of how personal information is collected and processed and used within the scope of normal business activities. 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 with 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 aspect of a privacy concern that needs to be addressed when they adopt a cloud technology solution. Fernandes et al. (2014) point out that the state of privacy in cloud computing is unstable and not yet well understood. Organizations need to develop responsible privacy practices (Boritz and No, 2011). Toy and Hay (2015) call for more research in the area of privacy auditing along the topic areas of effectiveness of privacy audits and the value of privacy audits from stakeholders perception. 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 personally 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?

To effectively develop privacy policies and practices such as a privacy governance policy, a privacy strategy or privacy assurance practices for cloud computing organizations need to define a set of guiding privacy objectives that can be applied across their organization. The purpose of this research is to enhance cloud privacy through the understanding of individual internal values towards privacy within cloud computing environments. For the purpose of this study, we adopted Keeney’s (1994) value-focused thinking (VFT) approach to identify privacy objectives with respect to cloud computing. This paper is organized into six sections. After this brief introduction, the second section provides a critical review of cloud privacy research literature frames the need for a better understanding of cloud privacy expectations. The third section describes the research method we applied to this study along with a discussion on our data analysis process. The fourth section presents the results of our analysis in the form of cloud privacy objectives. In the fifth section, our discussion will focus on the importance of the derived objectives with respect to the extant literature and provide a platform from which to establish their relevance and contributions to the overall strategic objective of ensuring privacy in cloud computing. The final section conveys our concluding remarks about the importance of ensuring cloud privacy, future research opportunities and limitations of this study.
Literature review
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. Clarke (1999) defines information privacy as the interest people have in controlling, or at least significantly influencing, the handling of information about themselves. 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. Privacy concerns continue to hamper users who out-source their private data into the cloud storage (Hashem et al., 2015). Dinev et al. (2009) espoused that new technologies have strongly impacted our “privacy expectations” by changing how we interact with each other online and how information is generated, shared and distributed. In essence, the contextual aspects of how users are interacting with each other are changing and so is their view of privacy because they are experiencing new threats. Even the notion of privacy itself has been found to change depending on the nature of its threats (Sheehan, 2002). Organizations are finding it difficult to manage their privacy policies and practices in the cloud because of the uncertainty of privacy expectations.

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) raise the concern “that the speed and flexibility of adjustments to vendor offerings that benefit business and provides a strong motivation for the use of cloud computing might come at a cost of compromise to the safety of data” (p. 133). 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 generate the majority of revenue for cloud providers; therefore, it is in the interests of the advertisers that dictates how privacy issues are or are not resolved. Additionally, 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 are important for easing privacy concerns and building user trust (Katzan, 2010).

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 (Gelman, 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). Gelman (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 Benamer, 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.

Our review of the 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. Additionally, we found a limited amount of literature that had a research focus on understanding individuals’ values and the usage of cloud computing or information privacy in the cloud. We argue that to ensure privacy in the cloud we first have to identify individuals’ privacy objectives, which are embedded in their values towards privacy. For this paper, we adopted a VFT approach to conduct our study of cloud privacy. This methodology will be discussed in great detail in the next section.

Research methodology
For this study, we adopted Keeney’s (1994) VFT approach to examine the issue of privacy in cloud computing. Several information systems researchers have used a value-focused thinking approach to develop objectives based on stakeholders’ values within a specific context domain. Dhillon and Torkzadeh (2006) used VFT to develop information system security objectives. Sheng et al. (2005) used value focus thinking to examine strategic implications of mobile technology within the publishing industry. Mishra (2015) used VFT to develop security governance objectives. We used Keeney’s three-step methodology to identify privacy objectives for cloud computing. This process involved eliciting individual values about cloud privacy and then systematically converting these into means and fundamental objectives.

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. 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 offer very limited information, 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. A fundamental objective is 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. To classify the objectives and to establish their relationship researchers ask the question of “Why is this objective important?” (WITI test), 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; therefore, it is considered to be a means objective. For example, the means objective to have the ability to minimize unnecessary access to information supports the fundamental objective to maximize identity management controls.

Data collection
For this study, we interviewed 90 individuals who had 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 per cent female and 58 per cent 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, which allowed for probing question techniques as recommended by Keeney (1994) to extract the latent values of individuals with regards to their privacy values. The average duration of the interviews was 40 min. Notes taken during the interviews were recorded directly after the interview to ensure that all the richness of the interview was captured and documented.

Organizing values to develop cloud privacy objectives
Once all the objectives have been sorted into either fundamental or means objective categories it is important to evaluate them to ensure their validity. There are many ways to ensure the validity of the results of a research study. Typically the means of validation depends on the type of research methods being used. To validate the individuals’ privacy objectives identified in this study, we decided to use a panel of experts as suggested by Emory and Cooper (1991). The criteria used for selecting the panelists was that each of the members should either have an interest in cloud privacy issues or have a job responsibility within the domain of auditing or using cloud technologies. The following is a description of the members on the panel and their IT experience.

• 1st panelist is a Field Service Engineer with eight 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;
• 2nd 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;
• 3rd panelist is an Information Security Officer at a large public university with 11 years experience in IT management;
• 4th panelist is a programmer analyst for a national healthcare provider with 10 years experience in the IT industry;
• 5th 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; and
These industry experts were used to evaluate the analysis of the VFT phase. 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 further classified as either a fundamental, or means objective. These objectives were then compared with each other to gain further insight in the context of ensuring privacy in cloud computing environments through the WITI test noted above. This process was repeated until all the main objectives were separated into fundamental objectives or means objectives.

#### Results

The results of our analysis resulted in six fundamental cloud privacy objectives and 19 Means objectives for cloud privacy. In our analysis, we 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 privacy objective being discussed. First we will discuss in detail the following the six fundamental objectives for ensuring privacy in cloud computing, that was derived from the value focus-thinking phase of this study:

1. increase trust with the cloud provider;
2. maximize identity management controls;
3. maximize responsibility of information stewardship;
4. maximize individual’s understanding of cloud service functionality;
5. maximize protection of rights to privacy; and
6. maintain the integrity of data.

Then we will discuss the 19 means objectives identified in our study as well.

### Fundamental cloud privacy objectives

**F1: Increase trust with cloud provider**

The relation between trust and privacy is an important topic that has been examined in the information systems literature from many different perspectives. Wang et al. (1998) reported that the most critical issue identified by internet customers is a fear and distrust regarding the 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.

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 panel experts 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.

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 underutilization 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.

Privacy and trust issues have been considered a major deterrent to the adoption of cloud computing (Pearson and Benameur, 2010; Buyya et al., 2009; Jaeger et al., 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 toward their handling of personal identifying information that permits meaningful accountability should be emphasized because it augments user’s trust, thus his/her conviction to use that cloud provider (Pearson and Charlesworth, 2009). 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 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 (Gopalakrishnan, 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 (Gopalakrishnan, 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 non-repudiation, 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 et al., 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 be able to determine what information is being shared with which parties and for what reason. Other concerns regarding the protection of personal identifying information also emerged in this study such as ensuring the protection of an individual’s right to anonymity, being informed when personal identifying information has been breached. These concerns are in line with prior research call for an efficient and effective privacy-preserving system for managing personal identifying information (Angin et al., 2010). 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 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.

F3: Maximize responsibility for information stewardship
While the 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. 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 that 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 toward the responsibility of protecting personal information.

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). 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.

F4: 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). From this, it is not too 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 to attract concerned users.

From a user’s 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 to use 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.

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.
A general assessment from this study 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 to attract concerned users. Therefore, 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.

F5: Maximize protection of rights to privacy

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 USA as to what privacy rights exist within US legal system in regards to the protection of personal information. 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. Mason (1986) supported the claim that individuals have the right to keep information about them private, to assure that it is accurate, maintain ownership of it and to have access to it. 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.

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, to assure that it is accurate, to maintain ownership of it and to have access to it. 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 expressed 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, a good example of one is when IBM initiated its Four Principles of Privacy to protect privacy rights of employees (Carroll, 1991). Drucker (1964) expressed that it is good business for corporations to be socially responsible. Along similar lines, Straub and Collins (1990) argue that the main concern for all managers should be deciding how they collect and disseminate information on individuals while respecting individuals’ rights to privacy. However, explicitly defining who has the legal right to individuals’ personal information is a bit challenging. 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. This ambiguity is compounded by the uncertainty of privacy regulatory requirements for cloud computing. Researchers 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). Therefore, 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 maintained on the cloud resources.

F6: 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 et al., 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 my 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 risk to data integrity in cloud computing is the threat of commingling of data (Zhou et al., 2010). When data from one organization is combined or commingled with data from another organization in the cloud, then it is much more vulnerable to being corrupted. 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 et al. (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.

**Mean objectives for cloud privacy**

*M1: Maximize effectiveness of secure data transfers*

Secure data transfers should be a concern for all of the traffic traveling 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.

Another participant stated they believe that “Data should be encrypted when it is transferred between vendors.” 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. This is because the simplest way to increase privacy protection is to encrypt its data before sending it to the cloud. 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 (Itani, Kayssi, and Chehab, 2009). It is important that cloud service providers understand the importance of clearly establishing well-defined secure data transferring practices.

*M2: 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 researched over the past decades (Rogers, 1962; Hernandez and Mazzon, 2007; Eriksson et al., 2005; Venkatesh and Davis, 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 or type of technology would be free of effort (Davis, 1989). While ease of use may be good for technology adoption careful consideration needs to be given the design of cloud computing applications to ensure that it is supporting strong privacy controls and not weakening the privacy environment. 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.
Feigenbaum et al. (2002) identified a critical concern with privacy-enhancing technology to be the apparent tradeoff between ease-of-use and security. 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.

M3: 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 that:

- There is an increased risk of being hacked when using the cloud.

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 et al., 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 built into all aspects of business processes whether they are technical or social-technical.

M4: 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 et al., 2006). Madden et al. (2007) found that 85 per cent of adults surveyed believed it was “very important” to control access to their personal 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, “I like it when I have the ability to set controls as to who can view my information.” Who should be allowed to access personal information has been an ongoing debate within the privacy literature. This is a question not only of technological constraints but also of organizational policy (Smith et al., 1996). Pearson and Charlesworth (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 cannot 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.

**M5: 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 EU and the USA approach to privacy protection. 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 guidance or rules for protecting privacy in cloud environments.

While the creation of cloud standards will go a long 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. Charlesworth (2009) cloud service providers will have to review and improve their privacy standards on an ongoing basis. Tang et al. (2008) 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 et al., 2011).

**M6: 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 per cent of all enterprises will revise their corporate privacy policy requirements to reflect changes in business practices, such as the use of cloud computing and location-based services available on a smartphone. From a user’s perspective, privacy risks vary significantly depending on privacy policies established by the cloud provider (Subashini and Kavitha, 2011). Pearson and Benamer (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.

A participant in this study has expressed concern 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 beforehand.

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 et al., 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 align their privacy policies and policy statements with their customers’ privacy values.

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 et al., 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 et al., 2005). Thus, it can be important to the bottom line of an organization to align their privacy policies and policy statements with their customers’ privacy values.

**M7: 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. 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 me that I 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.

Once a risk has been identified it is important to define acceptable use cases and necessary compensating controls before implementing a cloud-based solution. 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 Guinaliu (2006) claimed that clearly communicating privacy statements, security policies and risk assessments are effective methods for establishing trust in online service providers.
M8: 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 the 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 their history regarding how many times they have been hacked or the number of times their systems have crashed and for how long was it down.

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 reduced. 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 personally identifiable information. To maintain trust relationships with their users it is important that cloud service providers uphold 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 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.

M9: 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 am concerned my information could get in the wrong hands, even if they are employed by the company. I think that a thorough background check should be required before hiring new employees who have access to my information.

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 an 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.

**M10: Minimize government access to information**

Recent government actions towards the confiscation or seizure of cloud servers have heightened 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. Individuals’ concern about government seizure of cloud storage servers is less about protecting their illegal activity and more about protecting their privacy. Individuals have mixed feeling with regards to government’s 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 made the following claim:

> I am concerned 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.

**M11: 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 used privacy seals to install trust by verifying that the website has a policy about its collection and use of personally 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 request an audit of their cloud service 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.

M12: 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 (Kaufman, 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 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 and Samarati (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.

M13: 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 acknowledgment 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.

Ensuring proper controls surrounding personal data segregation also emerged in our discussions with our study’s participants. 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 and Kavitha, 2010).

**M14: Minimize third party access to information**

Limiting third party access to personal information is at the very core of the definition of personal information privacy. Personal information privacy has been defined as the ability of the individual to personally control information about oneself (Stone et al., 1983; Milberg et al., 1995). Individuals in this study have 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 they (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 access to their data files.

**M15: Minimize liability concerns**

Cloud users need to be 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 government I may be held responsible.

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.
M16: Ensure cloud service provider has effective internal controls

Maintaining protection of data and privacy required by current legislation in cloud computing is challenging. 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. Jansen and Grance (2011) 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.

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 to running a ‘well-oiled’ business. COSO’s Internal Control-Integrated Framework defines internal control has a process designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- effectiveness and efficiency of operations;
- reliability of financial reporting; and
- 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, risk assessment, information and communication, control activities, monitoring. Management needs to consider these five items 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 they can effectively implement privacy controls necessary to protect the user’s personal data and provide evidence about the effectiveness of those controls.

M17: Maximize availability of cloud resources

Having the ability to control access to one’s personal information is an 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 to access, it will impact the cloud users’ perception about the controls or lack of proper controls of the cloud service provider. A primary concern with the loss of availability to information stored in the cloud is that the user will lose trust in the cloud service provides ability to maintain control of their systems. Therefore if the cloud service provider cannot assure access to the users’ information how can they adequately protect their information or privacy. Managing trust perceptions such as these is an important aspect of managing consumer privacy concerns (Campbell, 1999). While it is impossible to guarantee 100 per cent 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.
M18: Increase awareness of data ownership

The distributed nature of cloud computing is changing the notion of 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 needs to be considered when implementing a cloud strategy.

With respect to this concern an individual expressed the following:

I believe I should have more control and the right to my own data even when using the cloud.

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).

M19: 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 me that I have a contract with the cloud service provider which ensures 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 experiencing rapid growth or are unsure of the what their computing infrastructure requirements will be like in the future due to the variable and unpredictable technology demands. However, in their analysis of cloud providers’ service contracts, they noted that the flexibility offered by Cloud computing is offset by uncertainty for the customer in terms of the location of data and the legal foundations of any contract with the provider. 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. 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 included in the negotiated service agreement. 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.

Discussion
Threats to privacy are a major concern for business leaders today. These privacy concerns are compounded in cloud computing environments due to the pervasive nature of how personal information is collected, process and used within the scope of normal business activities. Privacy threats to an organization using a cloud service come in many forms, 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. However, 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 required to instill public trust in a company’s 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 et al., 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 et al., 2002). Within the increase trust with the cloud provider objective, there are several guidelines that help management to build institution-based trust measures. Maximizing the 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 a 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 using 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**

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
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). 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 study it is important to understand the theoretical stance of these various perspectives because they are the theoretical foundations used by information systems researchers to study information privacy.

This research study emphasizes the importance of understanding individuals’ values as a means to assist organizations in the assurance of 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 using 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. Also, we espoused the importance of conducting a cloud privacy audit on a regular basis to reduce cloud privacy risk. Finally, we recommend incorporating the cloud privacy objectives from this study as privacy audit criteria because it is important to use 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. 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 to their privacy management process.

**Limitations**
There are two limitations 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 effects on privacy awareness. As 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 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 opposed 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). 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, we independently converted a sample of the raw values into common form objectives. We then compared our results to ensure the common form objectives were a fair representation of the initial raw values. We continued this process until we converted all the raw values into common form objectives. This check and balance process was reiterated with the following steps in the VFT process as well.

**Practical contributions**

One practical contribution of this study is for the use of our results by 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 using cloud technologies. By designing a cloud privacy audit program to include items from this study 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 cloud privacy objectives to 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 cloud privacy objectives 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.

Theoretical contributions
Before discussing the theoretical contributions of this study it is best to first reiterate the importance that, for this research study, 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. 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 research, one main theoretical contribution is the identification and development the means and fundamental cloud privacy objectives. This results from this study provides a foundation for future researchers to understand and the complexities surrounding the concept of privacy in cloud computing.

Future research
There are many possibilities for future research based on the cloud privacy objectives developed in this study. 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-objectives 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. The cloud privacy objectives identified in this study could be used in a design science study to design a cloud privacy audit framework. A third research study could use an action research study where an organization that needs to have a privacy audit performed uses the design designed cloud privacy framework and implement a cloud privacy audit. While still another 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.

References


**Further reading**


**Corresponding author**

David Lewis Coss can be contacted at: cossdl@cofc.edu