INDIVIDUAL VALUES FOR PROTECTING IDENTITY IN SOCIAL NETWORKS

Completed Research Paper

Gurpreet Dhillon
Virginia Commonwealth University
301 W. Main Street, Richmond, VA
23284, USA
gdhillon@vcu.edu

Romilla Chowdhuri
Virginia Commonwealth University
301 W. Main Street, Richmond, VA
23284, USA
syedr2@vcu.edu

Abstract

Consequences of loss of identity are severe and abuse by criminal elements is a real threat. Any effort to institute identity protection controls requires a strategic focus where objectives of individuals need to be understood and established. In this paper we undertake an extensive study to develop individual identity protection objectives. Using concepts rooted in value theory and value-focused thinking, we define five fundamental and fourteen means objectives. Our fundamental objectives for identity protection include: Maximizing end user trust; Ensuring development of social networking ethics; Ensuring authenticity of user identity; Maximizing identity management to make social networks useful; Maximizing social networking infrastructure protection. Our means objectives range from protecting individual identity from commercial exploitation to private and public segregation of information and maximizing communication richness. All together the fundamental and means objectives ensure protection of individual identity in social networking environments.

Keywords: Identity Protection, Social Networking Environments, Values, Value-focused Thinking, Qualitative Research, Security.

Introduction

Protection of personal identity in social networking environments has emerged to be problematic. It was recently reported that in the US there was a 32 percent increase in loss of identity complaints (Levin 2013). Whatever be the magnitude of identity compromises, there is a need to understand what causes identity breaches and then systematically plan to ensure that such compromises are prevented. Based on Hitlin (2003), we argue that personal values are a building block for individual identity. Therefore, it is important to make such values explicit for an enhanced understanding of what individuals consider to be important for identity protection.

In this paper we present an analysis of personal values in the context of protecting individual identity. Gregory and Keeney (1994) have argued that it is important to consider individual values since deciding about what aspects of identity should be public or private is ultimately a tradeoff amongst the objectives. Gregory and Keeney propose value-focused thinking (also see Keeney 1992) as a means of collating individual values to develop objectives. Our research is also based on value theory concepts and we use the corresponding value-focused thinking (Keeney 1992) to systematically elicit and synthesize values to define objectives. Our research follows the same tradition as proposed by Keeney (1992), which is well accepted in the extant literature (for example see Keeney 1999; Dhillon and Torkzadeh 2006; May et al. 2013; Hedström et al. 2011). We believe that value based identity objectives will help social networking sites to plan better for the protection of user identity. The objectives will also allow users to evaluate identity protection mechanism provided by various social networking sites.

This paper is organized into six sections. Following a brief introduction, section 2 introduces the theoretical foundations of this research. Concepts pertaining to individual values and identity are discussed. Section 3 presents the research methodology, which includes a discussion of how individual values can be elicited. In section 4 social media objectives identified in this study are presented and discussed. These objectives are classified as fundamental and means objectives. Section 5 discusses the objectives and their utility in protecting identity in social networking environments. Finally, section 6 concludes the discussions and identifies future research directions.

Theoretical foundation

There are two bodies of literature that inform this research. First relates to the concept of values. Second relates to identity protection. In this section both streams of research are reviewed.

Individual Values

In this study we adopt Keeney's (1992) definition of values according to which values are ethical principles used as guidelines for evaluating choices. Values come in all forms- "ethics, desired traits, characteristics of consequences that matter, guidelines for action, priorities, value tradeoffs, and attitudes toward risk all indicate values" (Pg. 7). Researchers have argued that values are a cultural manifestation of beliefs that are important to a particular group (Schein, 1985a, 1985b). Many scholars argue that the values can be best explicated from indigenous groups (Leidner and Kayworth, 2006).

There are several mainstream information systems (IS) theories that are founded on individual values, both explicitly and implicitly. However, as Horley (2012) notes, "despite recognition as an important, potentially unifying construct within the social sciences and humanities, *value* lacks an overarching theoretical framework." In recent years some progress has been made. Tan and Hunter (2002), for instance, introduce the personal construct theory as a means to study values, particularly with respect to different conceptions of systems developers. Keeney (1999) and Torkzadeh and Dhillon (2002) have introduced the concept of *value-focused thinking* into IS research. However, a unified value theory is still a far-fetched call.

Hechter (1993) has also observed that scholarly research in values has been limited. This is because of several impediments - values in all forms are unobservable; there has been limited contribution from informing disciplines of economics, psychology and sociology; simple postulation of values sounds unreasonable since processes responsible for generating them are unclear. Hechter's call for *novel*

measurement effort for the definition of values is indeed a reflection of Fischhoff (1991). The adherents, such as experimental psychologists, economists, and decision analysts believe that a reliable set of individual values can be elicited by appropriately probing people. A researcher may have to apply inferences to generate a common set of values. In the context of decision sciences, Keeney (1992), Gregory and Keeney (1994) were perhaps among the earlier scholars to define a theoretical basis for conceptualizing what values are and how these could be defined. In the IS literature, Torkzadeh and Dhillon (2002), Dhillon and Torkzadeh (2006), May et al. (2013), among few others, have illustrated how value theory concepts can be applied and used to define objectives, model constructs and develop appropriate measures. In this research we use the value theoretic concepts based on Keeney (1992) and other IS scholars. If values could explain the ideology of identity, social networking sites could use it to design protection mechanisms based on fine-grained value based priorities.

Identity and Identity Protection

In the literature several perspectives of *identity* are noted. Stryker and Burke (2000) classify and present three different variations. While some relate identity to *culture*, others consider identity as a *social association to a group*. Identity is also considered from a *multi-role* perspective. Regardless of the variations, Identity theory by itself finds its roots in symbolic interactionism (Mead, 1934; Blumer, 1986). The epistemological assumptions underlying symbolic interactionism rest on the assumption that the behavior exhibited by people is in effect a result of social interactions and interpretations. Thus, relatively speaking, *identification* is a social phenomenon embedded in the shared sense of belonging to a network that a person is associated to and becoming a part of those networks is a matter of choice dictated by the interpretation that a person draws outside the network. This view is consistent with Stryker and Burke (2000), as they note "… social structures outside given social networks act as boundaries affecting the probability that persons will enter those networks."

Several mechanisms link values and identity. In the literature Hitlin (2003) has defined a framework that links values to the core of personal identity. A comparison is drawn between the characteristics of values and identities. Both values and personal identities are concepts or beliefs, pertain to behaviors, transcend specific situations, guide the choice of behavior and events and are ordered by relative importance (Schwartz, 1992; Hitlin, 2003). In this paper we analyze the traits of personal identity protection. Following Hewitt (1997), personal identity emanates a sense of "individual autonomy rather than communal involvement." Identity protection then is a complex of individual values regarding protection of the autonomous self.

Recent trends in sharing personally identifiable information on the web, and its repercussion on identity have attracted the attention of many researchers (see Milne et al, 2004, Stutzman, 2006). Over the years while the magnitude of identity loss and its consequences has increased, the understanding of fundamental issues pertaining to identity and identity protection remains limited (Newman and McNally, 2005; White and Fisher, 2008). In the context of social networks identity protection has been considered problematic. This is largely because the boundaries within which individual autonomy (i.e. identity) is to be maintained have gotten transformed. As McQuail (1991) argues, the formal organizational structures and channels for information flow suggest a certain value structure to the manner in which we treat our identity. However, when these structures and channels get diffused or transformed or keep evolving, the individual values with respect to identity protection have no bearing (see McQuail, 1991). The confusion caused is typically at three levels: **1)** Confusion about personal values as to what is identity; **2)** Concern about how identity is protected by various institutions; **3)** Inability of the institutions to appreciate individual values regarding identity protection. This defines the scope of our current research and hence we set out to identify individual identity protection values in the context of social networking. We then convert the values to objectives that can be used to guide individuals and organizations. What we found and how we undertook the study is presented in subsequent sections.

Research Methodology

As noted earlier, in this research we use value theoretic concepts from Keeney (1992) to articulate the values and define objectives. Keeney argues that values are the guiding principles for decision-making. "…we should spend more of our decision-making time concentrating on what is important: articulating

and understanding our values and using these values to select meaningful decisions to ponder, to create better alternatives than those already identified, and to evaluate more carefully the desirability of the alternatives" (pg 3-4). Building on this premise, we believe a value-focused inquiry to elicit the identity protection objectives will help social networking sites to strategically plan for identity protection. It will also help users to assess the desirability of social networking sites with respect to the identified objectives.

Fischhoff (1991) argues that it is stakeholders who are in a position to articulate the values. So, in the context of social networks, it is individuals involved in online social engagements who might have an opinion or a perspective as to how their identity should be managed. Fischhoff also notes that three guiding principles define value articulation. First, the subjects are given enough time to think through questions during an interview. In case the subject struggles in framing a response, suitable probes be introduced (e.g. how can one protect his or her identity? What measures do you take to prevent leakage of financial information?) Second, the aim of value elicitation is to identify the comprehensible set of consequences, which helps at a later stage to define the objectives. The objectives themselves need to be commensurable into a common set. Third, there is a need to have diversity amongst the subjects. This means the sample respondents (or interviewees) need to be from different walks of life, which will allow multiple perspectives to be incorporated into the value set.

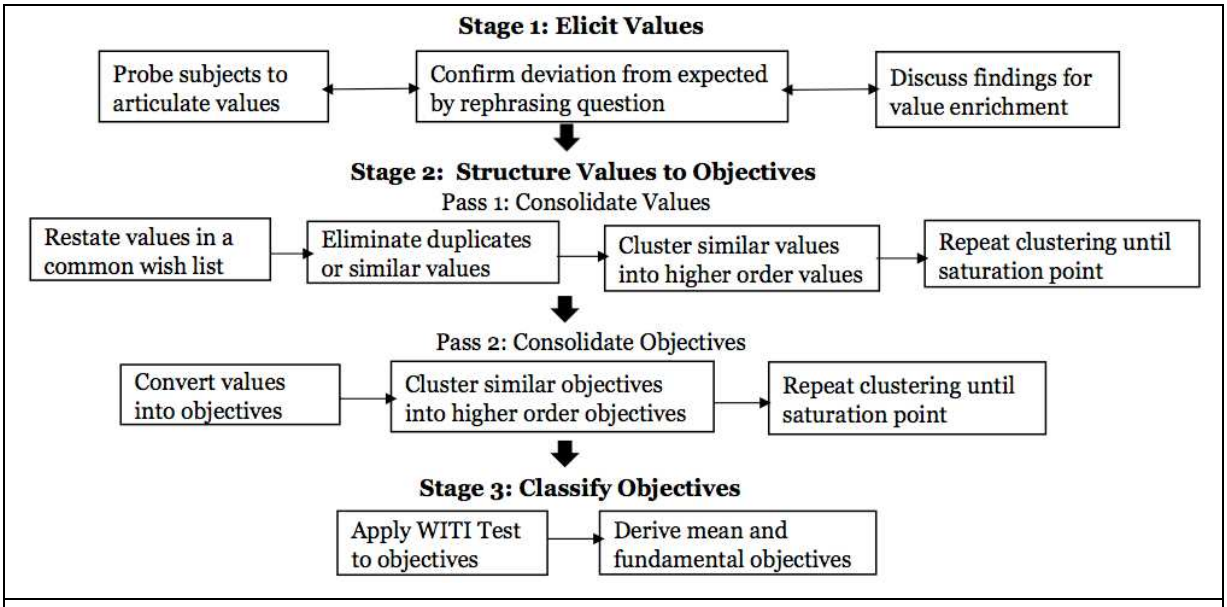

Figure 1. Data Collection and Analysis Process

Data Collection

The objective of this study is to identify individual values for identity protection. We sought typical social networking users to elicit their values. Our intention was to identify a large number of users who would fit an average profile. We used McCracken (1988) as a guide to select interviewees. Our starting point was to recruit working executives participating in a continuing education program at a large US based University. The candidates were recruited based on their age, gender and years of experience in using social networking. Our respondents, all located in the US, had an average age of 35 years (20-25 years: 35 respondents; 26-35 years: 40 respondents; 36-50 years: 40 respondents; 50 and older: 32 respondents). Nearly 52% were women and 48% were male. Average user experience in using social networking was 3 years with at least 2 active social network memberships. On average each user visited a social networking site at least twice a week for either personal social reasons or for business and other professional purposes. A total of 147 interviews were conducted between January 2012 and November 2012. Each interview lasted an average of 90 minutes. All interviews were recorded. Source files are available from the authors.

The project was undertaken following approval by the Institutional Review Board. The respondents were asked to think freely as to what they thought was important (or wished) for protecting their individual identity in the context of social networking. Suitable probes were used to uncover the latent values. The complete research process is shown in figure 1.

Data Analysis

Data collection and analysis followed the methodology proposed by Keeney (1992). It involves three stages - the identification and structuring of values followed by classifying objectives into fundamental and means. Following Keeney, we converted interview data into *common form values*, which were then clustered and redundancies were removed. A total of 147 interviews resulted in 2029 raw values, which after eliminating redundancies were reduced to a total of 1597 clean values. These were further consolidated, largely based on values emanating a similar meaning, to a total of 895 values. Each of the values was then converted into an objective. Keeney (1992) suggests adding a directional preference in forming the objectives. There is typically a many to one relationship, i.e. many values may result in one objectives. In a final synthesis we defined a total of 83 objectives. These objectives were clustered into 19 categories of objectives. As suggested by Keeney, we then employed the *Why It is Important Test (WITI)* test to classify the clusters into 5 fundamental and 14 means categories of objectives. Space limitations forbid us from describing the method in great detail, however we strictly adhered to Keeney (1992) in conducting this research. The process of creating objectives from values is exemplified in figure 2.

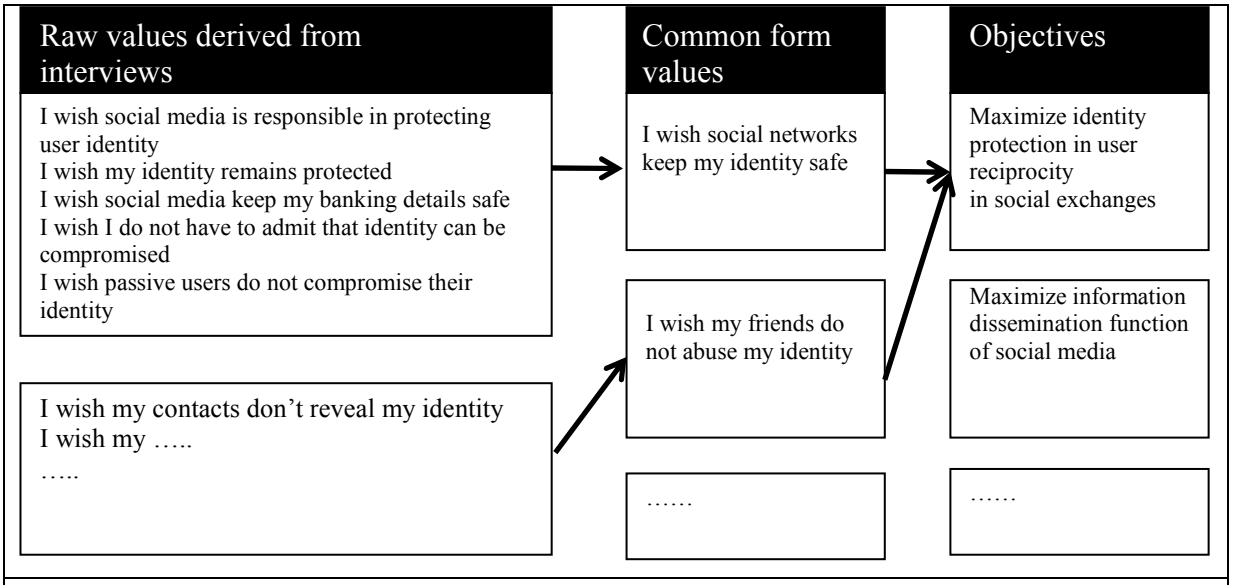

Figure 2. Illustration of creating objectives (only partial details are shown)

Social Media Objectives

In this study we defined 19 clusters of objectives ('clusters of objectives' are simply referred to as 'objectives'), which were divided into 5 fundamental and 14 means categories. The fundamental and means objectives appear in table 1.

Fundamental Objectives

The fundamental objectives defined in our study include: *maximize end-user trust*; *ensure development of social networking ethics*; *ensure authenticity of user identity*; *maximize identity management to*

make social networks useful; *maximize social networking infrastructure protection*. When considered collectively, it is interesting to note that our objectives suggest that any social networking identity protection initiative needs not only to focus on a well-designed infrastructure, but also on ensuring an ethical and a trusting environment.

Maximize end-user trust

Individual identity and trust are inter-related concepts. The social psychology literature considers identity to be some sort of a "theory of self" (see Stets and Burke 2000). This is where an individual asks some rather basic question - "Who am I?" Who do I want to be?" "What is my relationship with others?" The perception that an individual has about oneself and others introduces the concept of trust, which many consider a "social glue", which encapsulates the notion of "willingness to be vulnerable" (see Atkinson and Butcher 2003). The notion of vulnerability suggests that there is something important that is going to be lost. In our study, end-user trust emerged to be a fundamental objective. Even the values emanated by our respondents seemed to suggest an intricate relationship between identity and trust. As one of our respondents noted:

> I place a lot of trust in social media and am willing to let go of my personal identity. However, I do so only for websites that I trust. I do feel vulnerable though, especially when people can see my activities and my clicks on LinkedIn.

Ensure development of social networking ethics

In the literature there is a reference to a "privacy paradox", where individuals are willing to give up personal information simply to be part of a social networking site. Barnes (2006) narrates an instance where one of her students felt concerned about revealing personal information and yet her Facebook profile listed her home address, phone number and pictures of her young son. Issues related to private versus public space are central to any discussion on social networking ethics. However, apart from the obvious calls for increasing awareness or protecting children from predators, not much progress has been made. Light and McGarth (2010) have recently commented on the body of research commonly referred to as "disclosive ethics" and make a call of exploring ethics as defined by social networking technologies. Light and McGarth explore the human-centric focus on ethics and argue that technology mediates the meaning it carries. As an illustration, they note that the technology (Facebook) begins shaping behavior the moment an individual creates a profile. One of our respondents succinctly captures the complex interplay between social networking technology and ethics when she notes:

> Look at the teenagers. They interact with social media differently than the adults. This is because they have grown up with this new technology. Facebook, LinkedIn, and other such sites have potential to create disorders in people's lives. Many become emotionally weak. A friend of mine divorced her husband because she was not traveling or had a house like her other friends. I would simply blame it on the application TripIt!

Ensure authenticity of user identity

Authenticity of user identity on social networking sites is emerging to be critical. However, there are two confounding issues. First, the concept of identity as proposed by social networking sites is in conflict with user self-presentation strategies. The fixed nature of the profile is really not the way users behave in the real world. In an interesting piece of research, Paulhus et al. (1995) note that users systematically manipulate their self-presentation strategies to emanate the best profile. Second, social networking sites by nature de-contextualize relational ties and the broader social structures. The normative pressures of the wider real life social network become invisible and get replaced by a formalized social structure, albeit virtually. This results in individuals commodifying rather complex relationships (see Wee and Brooks 2010). Traversing the notion of *self* and *identity*, *self presentation* and *commoditization of identity* were captured by our respondents. One respondent in particular mentioned:

> I am really concerned as to how I am perceived in the virtual world. So, I restrict information, use multiple addresses, and hide certain details. Among friends I don't care. Among co-workers and others it is a serious matter. They need to see my best side.

Another respondent noted:

> Social networking sites are rather simplistic. They impose one profile onto you. The result is that we either fake it or just have multiple accounts.

Table 1: Fundamental and Means objectives for identity protection (all sub objectives are not shown)

Means Objectives	Fundamental Objectives
M1. Maximize individual identity in commercial exploitations of social media M2. Maximize safeguards for vulnerable people M3. Maximize authenticity of content M4. Maximize identity protection in context of single sign on M5. Maximize correspondence between individual and corporate identities M6. Maximize sensitivity of managing identity in different cultural settings M7. Maximize communication of identity protection measures M8. Maximize identity protection in information exchange M9. Maximize ease of use of controls (with partial list of sub-objectives for illustrative purpose)* *M9.1 Ensure users are able to customize privacy and identity* *M9.2 Ensure controls are intuitive to use* *M9.3 ....* *M9.4 Maximize automation of privacy settings* M10. Maximize private and public segregation of information M11. Maximize regulatory controls to protect user identity M12. Maximize forensic measures for identity protection M13. Maximize awareness of identity management in social networks M14. Maximize communication richness in social networks	F1. Maximize end user trust F2. Ensure development of social networking ethics (with partial list of sub-objectives for illustrative purpose)* *F2.1 Maximize definition of normative controls for* *F2.2 Identity management* *F2.3 .....* *F2.4 Discourage unethical consumption of information* *F2.5 Minimize profanity* F3. Ensure authenticity of user identity (with partial list of sub-objectives for illustrative purpose)* *F3.1 Ensure authenticity of members* *F3.2 Maximize integrity of individual identity* *F3.3 .....* F4. Maximize identity management to make social networks useful F5. Maximize social networking infrastructure protection

* Each cluster of Fundamental (F1-F5) and Means objectives (M1-M14) had several sub-objectives. In the table above only a sampling of these is presented (e.g. F2.1-2.5; F3.1-3.3 for Fundamentals and M9.1-9.4 for the Means).

Maximize identity management to make social networks useful

In an interesting article published nearly a decade ago (Wellman et al. 2001), the authors undertook an extensive study of 39,211 visitors to a National Geographic Society Web site to understand the social exchanges in an Internet mediated environment. While the study predates the advent of newer versions of social media, there are some interesting insights. Heavy reliance on the internet was found to be associated with participation in voluntary and political organizations. Interestingly the study also found that heavy users were perhaps the least committed to the online community. This finding is interesting in light of usefulness of social networks today. There is limited research though that evaluates behavior of people involved in social networks and how they evaluate usefulness. One of respondents succinctly put it as:

> Social Networks are like a reality show. We like seeing people enacting their lives. So, there is a fun and an entertainment value to social networks. I am unsure as to the extent of people's engagement in business. There seems to be significant value in terms of building relationships for the church and political causes.

Maximize social networking infrastructure protection

One of the biggest challenges in infrastructure protection is the *ripple effect*. What happens in one part of the infrastructure can have a cascading effect, directly and indirectly, on other parts, which can then impact large geographical areas (see Rinaldi et al. 2001). Social networks are emerging to play a more critical role in personal and business lives than ever before. For instance, the use of social networks in participatory surveillance (Albrechtslund 2008), intelligence gathering, health, and even Hollywood blockbusters (Asur and Huberman 2010) is abound. Given the increased dependence on the social networking infrastructure, it is, therefore, paramount to ensure its adequate protection. The security dilemma and the dependence on the networks is captured by one of our respondents:

> It is interesting that while social media (Twitter, Facebook etc.) are all for profit entities, yet we have become dependent on them for almost everything. At one level they really don't care about security and privacy, yet we can't seem to live without them. It is like the public utility companies, which have a clear for-profit mandate, and yet we trust them to operate ethically. Strong regulations is perhaps the answer.

Means Objectives

In addition to the fundamental objectives, we also define 14 clusters of means objectives ('clusters of objectives' are simply referred to as 'objectives'). A combination of all the means objectives forms the basis for protecting identity in social networking environments. In paragraphs below, we discuss each of these objectives.

Maximize individual identity in commercial exploitation of social media

The availability of active and a thriving online community has proven to be a great avenue for businesses to seek potential customers. However, in domesticating the social networking sites, users are confronted with a dilemma. The commercialization of personal information available on social networking sites has raised concern of exploitation of individual identity. Information exploitation occurs in two ways. First, user information is sought for direct behavioral targeting. For example, users are presented with targeted advertisements based on their preferences (Palmer and Koenig-Lewis, 2009). Second, user information is utilized to reach beyond their immediate networks. For example, using names and pictures of users to advertise or recommend products to their friends (Leskovec et al., 2007). Our respondents shared this concern as well. One in particular said:

> I definitely feel that they track when I see a sidebar listing some specific companies in my locality. The recommendations for shopping based on your preferences indicate that some big brother is watching.

Maximize safeguards for vulnerable groups

Social networking sites are indeed vulnerable for certain groups of people including children and adults (Miyazaki et al. 2009). Fear of identity theft among users is not only due to sheer ignorance but also due to the possibility of being exposed through other agencies. As one of our interviewees, who works with a not-for profit organization, expresses her fear in posting pictures of children on Facebook. Concerns for safeguarding vulnerable groups were voiced by many of our respondents. One in particular noted:

> I am worried about posting pictures of our children online. I have to do it for fundraising, but at the same time I am conscious about the gamut of risks I could be exposing them to. It is a virtual reality, which needs real responsibility.

Maximize authenticity of content

One of the biggest challenges of social networks is to determine validity of content. Part of the challenge is due to the fact that unlike focused blogs that are driven by topics, users drive social networks (Alan et al., 2007). Users publish information and share it with other participating users or networks. The ability of social networks to generate and distribute content faster than any other communication medium has created a kind of ripple effect in which validity of content gets lost. Essentially, incomplete information becomes available quickly to masses and is shared even before the facts are well established. This is captured succinctly by one of the respondents:

> Social networking sites enable us to post news instantly and make it available for everyone. It has affected the speed of business; one has to react quickly especially if the news is bogus and pertains to them.

Maximize identity protection in context of single sign on

Mushrooming of third party applications, such as games, surveys, polls etc. presents another threat to individual identity. While the intent of allowing access to third party applications via social media websites is appealing for businesses, the strategic alignment seems to ignore end-user perspective on identity. Narayanan and Vitaly (2009) voice similar concerns by stating that social networking sites indulge in breach of personally identifiable information by sharing it with third party applications without the consent or knowledge of users. One of the respondents echoed the concern:

> I will never access my banking sites through a social network. I am not sure if third party applications share the vision of identity protection of social networks. Moreover, third party applications may gather my information from different sources and then make it available for others at a petty price.

Maximize correspondence between individual and corporate identities

Identity is a slippery concept that assumes a sense of oneness and difference at the same time (Citrin et al., 2001). Hence, identity integrates as well as divides people. Citrin et al. state that one needs to understand the basis of categorization of identities. And while people can possess multiple identities, overlap between these identities can vary. Moreover, the significance of different potential identities and the behavior exhibited may vary as well (Thoits and Virshup, 1997). In the context of social networking sites, our participants express the need for different identities. The profiles could have little to no correspondence and hence provide flexibility to people exhibiting different personalities. However, as argued in the social psychology literature, existence of different identities leads to conflict, which essentially occurs when a person faces difficulties in reconciling the incompatible identities as each one entails a different behavior (Baumeister, 1986). The individual feels psychologically torn between multiple identities and hence may even fake or betray a few of the identities. In this context, the ability of having multiple identities in same or different networking sites not only makes one to question the legitimacy of behaviors exhibited but also the psychological stress it may exert on an individual. The participants in our study seem to be aware of identity conflict as one of them expressed:

> I connect only with people to whom I have to show my true self. I exchange some information online, as I would share offline. Managing one face on all forums makes me look professional.

Maximize sensitivity of managing identity in different cultural setting

The boundary-less communication platform that social media aims to provide is driven by an assumption of cultural homogeneity. Culture has been an interesting variable to explore in Information Systems research as IT and culture have always been at odds with each other. In a related article, Leidner and Kayworth (2006) undertake a value-based approach to the understanding of IT and culture. For the reconciliation of conflicts arising due to cultural differences, authors propose the reorientation of values. In the context of our study, for the elimination of cultural conflicts, social media networks would then require to reorient the values of identity. Since values are deep rooted in culture, it needs to be seen if the users hold on to identity protection over socialization. One of the respondents captured the essence of this conflict by stating:

> Social networking comes at a cost. What is considered to be sensitive and personal in one culture may be considered to be communal asset in another setting. I am concerned about my reputation, so I have to be not only considerate about implications of my own actions but also of my "friend's" actions.

Maximize identity protection in information exchange

Social networking sites are a lucrative source of personal information. As the popularity of the sites has increased, so has the attractiveness of criminals. In a study conducted by Bilge et al. (2009) the propensity of automated identity thefts and their relative ease is explicated. The feasibility of getting easy access to personal information is due to two reasons. One, the technical controls can be broken easily. For example, although sites provide CAPTCHAs*;* however, much more can be done to make them more robust. Two, users are not cautious when accepting connection requests or clicking on links. One of our respondents articulates the concern by stating:

> If I would be in the information stealing business, social networking sites are the place to start with. All I need is to get over the initial hitch of forming connections; access or inferring information would be easy. If a person doesn't state it, his or her connections will.

Maximize communication of identity protection measures

Ignorance isn't really bliss when it comes to identity management. One of the most common reasons of falling to the pitfalls of social networking sites is that the users are unaware of the technology they are using, and its implications for user identity. An interesting study is conducted by Qing and Dinev (2005) to understand reasons of apparent passivity and complacent behavior of Internet users towards spyware. It was found that awareness emerged as the most important factor that impacts user behavior in terms of measures taken to protect themselves against spywares. Our study corroborates the findings in the realm of identity management. Participants recognized that there is a need to increase awareness about social media and the measures that could be taken to protect against identity issues on these networks. While the responsibility lies more on users to protect their information, social networking sites also need to promote awareness about the technical controls and privacy policies. The essence of this objective is captured in the quotes of one of the social media users, who said:

> Targeted marketing and even recommending a product, because one of my connections liked it is nothing but hacking personal information. Most of the users are not tech-savvy and social media may get around by saying that they have provided the controls. I think the responsibility resides both with providers and users.

Maximize ease of use control

Pew research center, in a study[1] conducted in 2011-2012, reports that 83% of social media users fall in the age group of 18 to 29 and 32% are above 65 years. Moreover, out of total 67% internet users who use social networking sites, 66% have attained less than high school or high school level of education. Given such young and under-educated users, it becomes important that controls to protect individual information should be easy to use. Moreover, several studies have shown the impact of user perceived ease of use on the successful adoption of technology (Davis et al. 1989). In another study by Daugherty et al. (2005), perceived ease of use is conceptualized as self-efficacy for Internet based technologies. The participants in our study seem to be cognizant of this fact as one of them notes:

> One has to know how to control personal information. While there have been some sites that require a user to write HTML scripts to customize, automation would certainly increase ease of use.

Another elderly participant notes:

> My daughter taught me how to use the controls. Now even if I forget, I watch videos and can manage my account settings by myself. The controls are quite intuitive.

Maximize regulatory controls to protect user identity

A study by Edwards and Brown (2009) found that law, technology, and user desire to self-disclose are at odds with each other. Security of personal information in social networking sites is irreconcilable with user preferences and technological convenience of sharing it. As the authors put it, the fundamental issue is that social networking sites are neither regulated by law nor informed by user preferences but rather run by technology itself. Similar concerns related to copyrights, disclosure rules, and information censure, are echoed by our respondents, who note:

> There is a need for implementing regulations in Internet in general and social networking sites in particular. Social networking sites may appear to promote their own terms and conditions but the enactment is sporadic at best. They may also change those terms to their advantage if that serves their capitalistic interests.

Maximize forensic measures for identity protection

The knowledge and skills required to establish regulations and controls around emerging technologies, such as social media, have not kept up with the technological advances. Just when we were beginning to become comfortable with various computer forensic techniques, social media and social networks pose new challenges. There are new forms of social media crimes that surface everyday. But the regulators and prosecutors are simply playing catch-up. As Rogers (2003) notes, cyber forensics helps to identify criminals whose identity may be known or unknown. In a social networking context however advances in cyber forensic techniques need to be made. Our respondents recognize this and note:

> Exhibition of illicit behavior on social networks is not unseen. Since the sites are accessible to all types of people, having a mechanism to monitor accounts and provide activity logs can keep a check on offenders.

Maximize awareness of identity management in social networks

Traditionally identity management has been seen from a provider perspective. However, given the nature of information exchange in social networking sites, it is imperative that users take measures at their end as well. Besides being aware of controls and settings to protect individual identity, users also need to be

[1] http://pewinternet.org/Commentary/2012/March/Pew-Internet-Social-Networking-full-detail.aspx

cognizant of what information one should or should not be sharing on social networking sites. One of the findings of this study is that some people prefer to fake their identities as a protection strategy. However, fake identity could have many negative implications. Creating fake identity is a business of counterfeiters and perpetrators (Wang et al., 2006). Hence, it is important that users need to adopt legitimate means for protecting identity. One of our respondents reflected on the concern by stating:

> Although it is not required to provide personal information on social Networking Sites, but it is not difficult to interpret anyone's identity. To prevent compromise one can use a different identity altogether. However, at the same time I am worried if someone else uses my identity.

Maximize communication richness in social networks

Social networking sites are increasingly being used as mainstream communication platforms, both for personal and professional exchanges. Unlike traditional communication media, social networking sites enable communication in an ever-widening network. More than ever, the massive information production and distribution capability of social media has imposed additional responsibility on users – to be mindful of what they post and being responsible for their actions. The duality of social networking exists in allowing rich, real-time, asynchronous or synchronous communication and offering permanency of messages on one hand, and exposing individuals to various risks on the other. In a related study, Livingstone (2008) points out advantages and disadvantages that social networking sites pose. The dilemma is captured by one of our respondents:

> Social networking sites offer several advantages: one can broadcast, connect with old pals, send email faster, and reach out to the whole world. However, one should not ignore the inherent risks: information abuse, identity theft, unproductivity, obsession, and making yourself available to the criminal world.

Maximize private and public segregation of information

In a study, Constant et al. (1994) address attitudes that drive information exchange in an organizational setting. Individuals tend to share private information only with specific people and in certain settings. Information related to their ability to complete a certain task is shared in a specific manner. Similarly in a social networking environment, individuals like segregating their information and share only those aspects they believe they should. It is therefore important to design ability to not only classify different kinds of information, but also how this information is shared in a network. One of the respondents reflected on this requirement as follows:

> Information that is shared online is never going to be absolutely private; however, to avoid social tensions, I restrict visibility to my sensitive information to certain people whom I trust. Nevertheless, they have an ability to make my information public. So as a rule, I can either accept the risk or have the conversation in an offline setting.

Discussion

Keeney (1994) has argued that an organization's strategic objectives form the basis for various decision opportunities. Over the past several decades the link between strategic objectives and decision making and strategic planning has been well established (e.g. see Ansoff 1987, among others). However, even today many organizations do not have carefully organized strategic objectives, let alone their use in decision-making and strategic planning. As Keeney (1994) notes:

> How many organizations have carefully written down and organized their strategic objectives? In how many organizations do the employees know and understand the organization's strategic objectives? The answer to both questions is "very few." The chance to state and clarify these strategic objectives is itself a decision opportunity. Pg. 40.

In the context of protecting identity in social networks, there is a need to decide *what* needs protection, and *how* such protection can be instituted. As a user of social networks an individual may not have much control over what gets decided by a firm or how other individuals may behave. One stakeholder may want a certain alternative to be selected, while a different stakeholder may have the power to execute the decision. The government may want *regulatory control to protect user identity* in social networks. The social networking firm may want to implement *ease of use of controls*. An individual may want *segregation of private and public information*.

In a typical strategic planning decision context, there will be a need to have trade-offs amongst the objectives. For any given objective (say *O*), there would be a range of measures that describe a given objectives (say *X*). So the vector $X = (x_1, x_2, \ldots x_n)$ describes all the measures that define a given objective. The prioritizing of the objectives therefore provides a value model that suggests the overall desirability as (after May et al. 2013; Keeney 1999):

$$v(x_1, x_2, \ldots x_n,) = \sum_{i=1}^{n} k_i \, v_i \, (x_i)$$

where k_i is the weight that prioritizes the objective and v_i is the relative desirability. Given the multitude of identity protection objectives in social networking environments, it is but prudent to consider relative desirability and establish trade-offs amongst objectives.

The objectives and the value model are rather useful in improving or changing the manner in which identity protection in social networks in undertaken. If one is to find a gap in the various measures that define an objective, it presents an opportunity to make an improvement. For example, *maximizing ease of use of controls* contributes to *maximizing private and public segregation of information*, which in turn leads to *maximizing individual identity in commercial exploitation of social media*. If the built in controls are not easy to use, it becomes difficult for individuals to differentiate between public and private information and how such information can be segregated in an online setting. As businesses collect increasingly more personally identifiable information, it becomes difficult to prevent the commercial exploitation of the information, because what was supposed to be private ends up in the public domain.

It goes without saying that individual objectives relating to identity define how we operate in a social networking environment. What people share or intend to share and what information companies collect or aspire to collect is characterized by multiple and often conflicting objectives. Given a particular decision context, each of the objectives is a statement of what one wants.

Let's suppose you are a stakeholder who wants your decision maker to "maximize protection of individual identity in social networking interactions." At all times you should look for an opportunity to take control of the decision situation. Rather than allow a decision maker to chose an alternative such as "use of social media for communication", you should create alternatives that help in modifying your desired alternative (i.e. protection of individual identity in social interactions) such that its main features remain intact, and is better that than whatever the existing alternatives are. For instance, the decision maker can be convinced that using social media for communication may be a worth cause, but at the same time protection of individual identity in the social networking interactions needs to be maximized and integration of social media into conventional communication channels also needs to be maximized. By focusing on all these features, it would be possible for the decision maker to ensure (or maximize) communication richness in social networks. Thus, the definition of objectives helps all stakeholders to strategically plan for a positive outcome. The cluster of objectives used in the above example are drawn from the objectives identified in our study and the one particularly used here is:

Maximize communication richness in social networks
- Maximize use of social media for communication
- Maximize protection of individual identity in social network interactions
- Maximize integration of social media with conventional communication channels

Conclusion

Value-focused thinking provides a logical means to identify and structure the objectives. Typically individuals are constrained by a given set of pre-existing alternatives, which define the way forward. The objectives for identity protection in a social networking environment are in many ways rather controversial. Opinions are usually divided amongst stakeholders. As McDaniels and Trousdale (1999) note, value-focused thinking affords a "simple but powerful form of *decision therapy* or even *organizational therapy*" (Pg. 68). In line with arguments proposed by McDaniels and Trousdale (1999), Keeney (1999), and others, when organizations are confronted with troubling scenarios, such as identity protection, focusing on what is important, particularly from multiple perspectives is helpful. Defining a strategic plan based on identity protection objectives is something that would indeed benefit all stakeholders immensely. While value-focused thinking is not without limitations, the fact that researchers were cognizant of the possible biases and carefully engaged in clustering the objectives helped in managing the possible limitations. The final set of fundamental and means objectives allow several avenues for future research. Similar to the work of Torkzadeh and Dhillon (2002), there are clearly opportunities to develop measurement instruments for assessing the level and extent of identity protection. This research can also adopt a design science approach to define audit frameworks to evaluate level and extent of identity protection offered in social networking environments.

References

Alan, M., Marcon, M., Gummadi, K.P., Druschel, P., and Bhattacharjee, B. 2007 "Measurement and analysis of online social networks." in *Proceedings of the 7th ACM SIGCOMM conference on Internet measurement*, ACM, pp 29-42.

Albrechtslund, A. 2008. "Online social networking as participatory surveillance," *First Monday* (13:3), p 3.

Ansoff, H. I. 1987. *Corporate strategy*, Penguin Books: Harmondsworth, UK.

Asur, S., and Huberman, B. A. 2010. "Predicting the future with social media," Web Intelligence and Intelligent Agent Technology (WI-IAT), IEEE/WIC/ACM Conference on, IEEE, pp. 492-499.

Atkinson, S., and Butcher, D. 2003. "Trust in managerial relationships," *Journal of Managerial Psychology* (18:4), pp 282-304.

Barnes, S. B. 2006. "A privacy paradox: social networking in the United States," *First Monday* (9:4).

Baumeister, R.F. 1986. *Identity: Cultural change and the struggle for self*, New York: Oxford University Press.

Bilge, L., Strufe, T., Balzarotti, D., & Kirda, E. 2009 "All your contacts are belong to us: automated identity theft attacks on social networks," in *Proceedings of the 18th international conference on World Wide Web, ACM*, pp 551-560

Blumer, H. 1986. *Symbolic interactionism: Perspective and method*, Berkeley: University of California Press.

Citrin, J., Wong, C. and Duff, B. 2001. "The Meaning of American National Identity: Patterns of Ethnic Conflict and Consensus" in Ashmore, R. D., Jussim, L. J., & Wilder, D. *Social identity, intergroup conflict, and conflict reduction (3),* Oxford University Press, USA.

Constant, D., Sara K., and Lee S. *1994. "*What's mine is ours, or is it? A study of attitudes about information sharing," *Information Systems Research* (5:4), pp 400-421.

Daugherty, T., Eastin, M., and Gangadharbatla H. 2005, "e-CRM: Understanding Internet Confidence and Implications for Customer Relationship Management," in *Advances in Electronic Marketing*, I. Clark III and T. Flaherty (eds.), Harrisonburg, PA: Idea Group Publishing, Inc., pp 67-82

Davis, F.D., R.P. Bagozzi, and P.R. Warshaw. 1989, "User Acceptance of Computer Technology: A Comparison of Two Theoretical Models," *Management Science (*35:8), pp 982-1003

Dhillon, G., and Torkzadeh, G. 2006. "Value focused assessment of Information System Security in Organizations," *Information Systems Journal* (16:3), pp 293-314.

Edwards, L., and Brown, I. 2009 "Data control and social networking: irreconcilable ideas?" in *Harboring Data: Information Security, Law and the Corporation*, A. Matwyshyn (ed.), Stanford, CA: Stanford University Press, pp 202-227.

Fischhoff, B. 1991. "Value elicitation: is there anything in there?" *American Psychologist* (46:8), pp 835-

847
Gregory, R., and Keeney, R. L. 1994. "Creating policy alternatives using stakeholder values," *Management Science* (40:8), pp 1035-1048.
Hechter, M. 1993. "Values research in the social and behavioral sciences," in *The origin of values,* M. Hechter, L. Nadel, and R. E. Michod (eds.), New York: Aldine, pp 1-28
Hedström, K., Kolkowska, E., Karlsson, F., and Allen, J. P. 2011. "Value conflicts for information security management," *The Journal of Strategic Information Systems* (20:4), pp 373-384.
Hewitt, J. P. 1997. *Self and Society: A Symbolic Interactionist Social Psychology,* Boston: Allyn & Bacon
Hitlin, S. 2003. "Values as the core of personal identity: Drawing links between the two theories of self," *Social Psychology Quarterly* (66:), pp 118–137.
Horley, J. 2012. "Personal Construct Theory and Human Values," *Journal of Human Values* (18:2), pp 161-171.
Qing, H. and Dinev. T. 2005. "Is spyware an internet nuisance or public menace?" *Communications of the ACM* (48:8), pp 61-66.
Keeney, R. L. 1992. *Value-focused thinking*, (Harvard University Press: Cambridge, Massachusetts.
Keeney, R. L. 1994. "Creativity in decision making with value-focused thinking," *Sloan Management Review* (35:4), pp 33-41.
Keeney, R. L. 1999. "The value of Internet commerce to the customer," *Management Science* (45:4), pp 533-542.
Leidner, D. E., and Kayworth, T. 2006. "Review: a review of culture in information systems research: toward a theory of information technology culture conflict," *MIS quarterly* (30:2), pp 357-399.
Leskovec, J., Adamic, L. A., and Huberman, B. A. 2007. "The dynamics of viral marketing," *ACM Transactions on the Web (TWEB)*, (1:1), pp 1-43.
Levin, A. 2013. "12.6 Million Reasons Why Identity Theft Matters," (available at http://www.huffingtonpost.com/adam-levin/126-million-reasons-why-i_b_2788870.html).
Light, B., and McGarth, K. 2010. "Ethics and social networking sites: a disclosive analysis of Facebook," *Information Technology & People* (23:4), pp 290-311.
Livingstone, S, 2008. "Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression," *New media & society* (10:3), pp 393-411.
May, J., Dhillon, G., and Caldeira, M. 2013. "Defining value-based objectives for ERP systems planning," *Decision Support Systems* (55:1), pp98-109.
McCraken, G. D. 1988. *The long interview*, Newbury Park, CA: Sage.
McDaniels, T., and Trousdale, W. 1999. "Value-Focused Thinking in a Difficult Context: Planning Tourism for Guimaras, Philippines," *Interfaces* (29:4), pp 58-70.
McQuail, D. 1991. *Mass communication theory: An introduction*, Barcelona: Sage.
Mead, George H. 1934. *Mind, Self and Society,* Chicago: University of Chicago Press.
Milne, G. R., Rohm, A. J., & Bahl, S. 2004. "Consumers' protection of online privacy and identity." *Journal of Consumer Affairs*, (38:2), pp 217-232.
Miyazaki, A. D., Stanaland, A. J., and Lwin, M. O. 2009. "Self-regulatory safeguards and the online privacy of preteen children," *Journal of Advertising* (38:4), pp 79-91.
Narayanan, A., and Vitaly S. 2009. "De-anonymizing social networks," in *30th IEEE Symposium on Security and Privacy,* IEEE, pp 173-187.
Newman, G. R., and McNally, M. M. 2005. "Identity theft literature review." *US Department of Justice*.
Palmer, A., & Koenig-Lewis, N. 2009. "An experiential, social network-based approach to direct marketing," *Direct Marketing: An International Journal*, (*3:*3), pp 162-176.
Paulhus, D. L., Bruce, M. N., and Trapnell, P. D. 1995. "Effects of self-presentation strategies on personality profiles and their structure," *Personality & Social Psychology Bulletin* (21:2), pp 100-108.
Rinaldi, S. M., Peerenboom, J. P., and Kelly, T. K. 2001. "Identifying, understanding, and analyzing critical infrastructure interdependencies," *Control Systems, IEEE* (21:6), pp 11-25.
Rogers, M. 2003. "The role of criminal profiling in the computer forensics process," *Computers & Security*, (*22*:4), pp 292-298.
Schein, E. H. 1985a. "How Culture Forms, Develops and Changes," in *Gaining Control of the Corporate Culture*, R. H. Kilmann, M. J. et al. (eds.), Jossey-Bass, San Francisco, pp. 17-43.
Schein, E. H. 1985b. *Organizational Culture and Leadership*, Jossey-Bass, San Francisco, CA.
Schwartz, S. H. 1992. "Universals in the content and structure of values: Theoretical advances and empirical tests in 20 countries," *Advances in experimental social psychology*, (*25:*1), pp 1-65.
Stets, J. E., and Burke, P. J. 2000. "Identity theory and social identity theory," *Social Psychology*

Quarterly (63:3), pp 224-237.
Stryker, S. and Burke, P. J. 2000 "The past, present, and future of an identity theory," *Social psychology quarterly*, (63:) pp 284-297.
Stutzman, F. 2006. "An evaluation of identity-sharing behavior in social network communities." *Journal of the International Digital Media and Arts Association,* (3:1), pp 10-18.
Tan, F. B., and Hunter, M. G. 2002. "The Repertory Grid Technique: A method for the study of cognition in information systems," *MIS Quarterly* (26:1), pp 39-57.
Thoits, P.A., & Virshup, L. K. 1997. "Me's and We's: Forms and functions of social identities." in *Self and Identity: Fundamental issues,* R.D. Ashmore and L. Jussim, (eds.), New York: Oxford University Press, pp 106-133.
Torkzadeh, G., and Dhillon, G. 2002. "Measuring factors that influence the success of Internet commerce," *Information Systems Research* (13:2), pp 187-204.
Wang, W., Yufei Y., and Norm, A. 2006 "A contextual framework for combating identity theft," *Security & Privacy, IEEE* (4:2), pp 30-38.
Wee, L., and Brooks, A. 2010. "Personal branding and the commodification of reflexivity," *Cultural Sociology* (4:1), pp 45-62.
Wellman, B., Haase, A. Q., Witte, J., and Hampton, K. 2001. "Does the Internet increase, decrease, or supplement social capital? Social networks, participation, and community commitment," *American behavioral scientist* (45:3), pp 436-455.
White, M. D., and Fisher, C. 2008. "Assessing Our Knowledge of Identity Theft The Challenges to Effective Prevention and Control Efforts." *Criminal Justice Policy Review*, (19:1), pp 3-24.