Online Social Networks: Enhancing user trust through effective controls and identity management

Ryan Galpin
Department of Information Systems
University of Fort Hare
East London, South Africa
rwgalpin@gmail.com

Stephen V. Flowerday
Department of Information Systems
University of Fort Hare
East London, South Africa
sflowerday@ufh.ac.za

Abstract - **Online social networking is one of the largest Internet activities, with almost one third of all daily Internet users visiting these websites. Characteristics of this environment are issues relating to trust, user privacy and anonymity. Service providers are focused primarily on acquiring users and little attention is given to the effective management of these users within the social networking environment. In order to examine this problem, user trust and its enhancement is discussed. An evaluation of current identity management processes and effective controls is undertaken, in order to understand the current environment. Lastly, by means of a detailed experiment focusing on the two main online social networking providers, Facebook and MySpace, controls and identity management processes were assessed for vulnerabilities. The findings of this experiment, together with the current environment of controls and identity management practices, form the proposed set of controls. These controls are aimed at increasing trust and privacy through the effective implementation of these controls and identity management processes.**

Keywords: online social networking, trust, privacy, identity management, Facebook, MySpace

I. INTRODUCTION

Online social networks are currently one of the most popular Internet activities, recently even eclipsing email usage. More than two-thirds of the global on-line population visit and participate in social networks, confirming its worldwide popularity [1]. Online social networking websites leading this trend are Facebook and MySpace, with Facebook presently leading the competitors with impressive usage statistics. The percentage of worldwide Internet users that visit Facebook is reported to be a monthly average of 32% [2]. That amounts to almost one third of all Internet users at a given point. In comparison, MySpace attracts only a monthly average of 3% [3]. Based on these statistics, online social networking is without question, a global phenomenon. Together with such a fast spreading activity, various concerns and risks become evident. The establishment of trust and the protection of users becomes an ongoing challenge within the online social networking environment, with the threat of misuse and privacy intrusions by malicious users illustrating this challenge. The identities encountered within these online environments are known as Virtual Persons. This Virtual Person serves as a mask for the real underlying identity, known as the subject. This subject can be real or fabricated, and can have multiple masks through which they interact [4]. Due to this degree of anonymity, online social network providers are tasked with maintaining a connection between the multiple users in the environment and the true identity of the individual they represent. The ability to accurately authenticate these identities requires a form of control that can map multiple users to their singular entity. The introduction of Identity Management (IDM) procedures and systems to the online environment serves as this control. In order for a trusting relationship to be formed between the users and the social networking service providers, controls and authentication procedures must be implemented to limit the occurrence of these malicious attacks. Currently, these controls are weak and the IDM procedures in place to protect users are inconclusive [5]. As a result of this inability of online social network providers to manage identities within this environment, users develop a lack of trust for the system and the services it provides.

A more serious concern for social networking service providers is that they are continually finding themselves as targeted platforms from which sexual offenders and various other individuals, intending to defame or harm users, launch their attacks. Numerous news and web articles highlight this problem and report on the thousands of offensive users being identified and removed yearly [30] [8] [10]. The personal risk associated with these types of attacks includes kidnappings, child molestation, sexual abuse, defamation and other forms of harassment and indecency [31]. In June 2008, a middle aged woman was charged with using MySpace to 'cyber bully' a 13 year-old girl who later, as a result of the abuse, took her own life. The woman allegedly posed online as a teenage boy and used this identity to interact with the girl [10].

It is therefore apparent that misrepresentation of identity within the social network environment is a serious concern. Trusting relationships are formed all too easily, resulting in the inexperienced or adolescent users falling prey to those wishing to inflict harm.

Due to these concerns and identified risks, the primary objective of this paper is to investigate how user trust can be enhanced through the implementation of effective controls and IDM practices. Elements that contribute to user trust within the online social networking context are also explored, together with an assessment of current IDM practices evident within the two main social network providers, Facebook and MySpace. The remainder of this paper comprises of the following sections. Section 2 provides an overview of online social

networks, and introduces the vulnerabilities and concerns associated with using the service. Section 3 defines the concept of trust and further explores the challenge arising when attempting to establish a trusting relationship between users and service providers. Section 4 provides an overview of the current forms of IDM, and defines their application to online social networking. Due to the nature of information that can be disclosed through online social networks, trust and the preservation of the trusting relationship is important. Section 5 introduces an experiment used to evaluate online social network providers' controls and practices, resulting in the identification of vulnerabilities. Finally, section 7 presents the set of controls recommended to ensure user security and enhanced levels of trust if implemented by online social networking service providers.

II. ONLINE SOCIAL NETWORKING VULNERABILITIES

In order to understand the vulnerable areas of online social networks, the security and privacy risks associated with using the social networking services will be presented. These will highlight the vulnerable areas evident within the online social networking environment.

A. Online Social Networks(OSN)

A typical social network provider offers several basic core features for users. The most basic of these features is the ability to create and share a personal profile. This profile page typically includes a photograph, some basic personal information (such as name, age, gender, and location) and other areas of interest. OSN enables users to interact and develop friendships with users anywhere in the world.

B. Vulnerabilities - Security and Privacy Risks

OSN are faced with two key security risks which can directly affect users and their interactions with the service providers. The first evident risk is that social network providers are unable to provide effective user authentication in assisting users to identify with whom they are interacting with [6] [7]. This is a result of the ease with which an individual can create a profile. No concrete identifiers are needed, and an email address is anonymous and easily created. Identity theft, impersonation and fictitious profile fabrication are common occurrences, as the natures of most online interactions are anonymous and untraceable. Due to this lack of authentication when profiles are created, imposter profiles can easily be developed to assume the identity of an individual. Figure 1 shows this complex nature of online interactions with an example of the partial identities of an individual.

An individual would typically appear under many partial identities within the real world, such as work, leisure and other dimensions of social interactions. Each of these identities exhibits characteristics about the individual, necessary for the chosen situation and also provides positive authentication of the individual. In an online encounter however, none of these characteristics can be authenticated, due to the anonymous nature of such interactions. To mitigate the user authentication shortfall, social networking providers suggest users spend time browsing the unknown friend requestor's friend list. If other common 'friends' and contacts are identified, a certain level of trust can be implied [9].

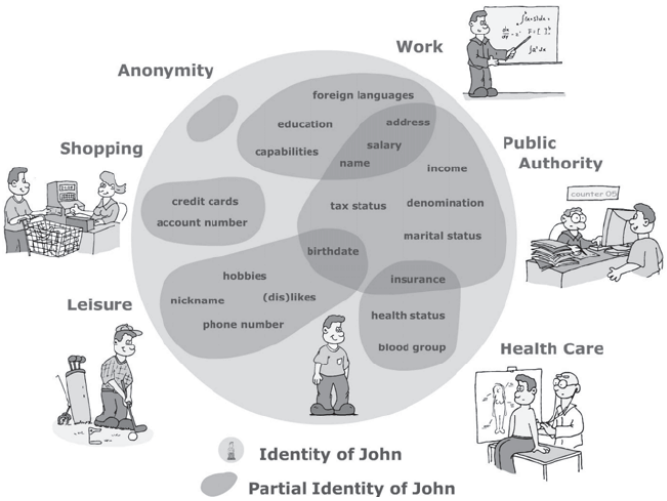

Figure 1. Partial Identities of John [9]

Currently, most OSN provide users with basic privacy functionality. This is designed to protect users from unwanted visitors to their profile page, with only accepted friends and network members able to view a user's complete profile. However, in order for this functionality to be effective, users should to be extremely selective when adding other users to their personal network or 'groups'. If all friend invitations are accepted without any scrutiny, there remains a possibility that one or more of these users may be sinister.

Based upon the security and privacy risks identified, online social networking users are vulnerable due to ineffective controls and IDM processes [5]. A basic understanding of current IDM processes is needed to recognize that effectiveness is lacking with current application of these processes. This will now be discussed.

III. INCREASING USER TRUST: THE CHALLENGE

Trust forms one of the most highly regarded human values and contributes to the basic pre-conditions when users adopt electronic based interactions [11]. The principles of trust evident in user relationships within online social networks must be explored to understand and define the expectations and requirements of online users within this online environment.

A. Trust and Online Social Networking

Trust can be defined as the willingness of an individual to be vulnerable to the actions of another individual, based on the expectation that the other will perform a particular action [12]. This acceptance of vulnerability and risk is irrespective of the ability to monitor or control the behaviour exhibited by the other party involved [13]. Another view defines trust as a mental phenomenon that occurs within social contexts and applies to both online and offline environments. Evidence that trust depends on previous experiences and not only on one-time interactions adds to the social context that trust develops gradually through interactions [14].

Within online social networking, trust and levels of trustworthiness within these websites can only be inferred based on the information available to users. It is evident that information influences people's judgements about others [14].

After users establish a membership and experience the social networking site as valuable, their usage of the site will increase. Each user will then have to decide if the posted information experienced on the social network is an honest reflection of reality. Before the evaluation of this information takes place, a user's perception of the safety and trustworthiness of these systems becomes influential. The assessment of an individual's trustworthiness is influenced by trust in the system and its users [11]. Online social networks provide individuals with an opportunity not experienced in real life situations. This opportunity is to view and analyse an individual's complete list of social references, which greatly influences levels of trustworthiness.

B. Trust and Uncertainty Reduction Theory

When undertaking an online social networking experience, individuals are faced with varying levels of uncertainty regarding the encounter. This is heightened when interacting during the introductory phase with unknown individuals. The unpredictable nature of these interactions adds to the feeling of uncertainty [15]. Trust and trustworthiness becomes a result of an individual's ability to reduce uncertainty by increasing an individual's behavioural predictability [16].

Uncertainty Reduction Theory is the discipline that defines the influence of uncertainty during a relationship, as well as a means of reducing this uncertainty and increasing the predictability of interacting individuals [17]. This is achieved by engaging in various steps and checkpoints to decide whether the individual is liked or disliked. In addition to this, communication and the exchange of information about individuals contributes to a decrease in uncertainty [18]. This theory applies well to the context of online social networking as all interactions take place between individuals. Several sources discuss the relationships between individuals, and the manner in which behaviour can contribute to trust and a lesser degree of uncertainty [15] [18] [17] [13].

Interactions between unknown individuals typically follow three stages [19]. Interaction may also terminate at the end of the entry phase, as continuing through the three stages is at the discretion of both individuals. Figure 2 illustrates these stages.

1 – Entry Stage	• Information – Demographic • Communication – following norms and rules
2 – Personal Stage	• Information – Attitudes, Values, Likes/Dislikes • Communication – more freely, less rules
3 – Exit Stage	• Information – less to none • Communication – future interactions

Figure 2. Three Stages Of Interaction (Own Compilation)

During the Entry Stage, information of a demographic nature is generally discussed. This includes name, gender and age, economic and social status. Interactions within this entry stage are controlled by societal communication rules and norms. When individuals begin to share information regarding attitudes, values and more personal data such as likes and dislikes, they have entered into the Personal Stage. During this stage, individuals feel less inhibited by rules and norms and have a tendency to communicate more freely with each other. Next is the Exit Stage. During this stage, individuals decide on future interaction plans. They may also discuss ways to allow the relationship to grow and continue.

C. Trust and controls

It is evident that trust and levels of trustworthiness are characterized by relationships between individuals. However, trust must also be placed in the system. Uncertainty is present in both elements of the encounter, so a way of reducing this uncertainty and increasing user confidence is needed. The level of trust and the presence and adequacy of controls are the two main factors affecting user confidence. This is depicted in Figure 3. The higher the degree of trust displayed between individuals, the less need to implement stringent controls. This can be reversed if a low degree of trust is evident, where more controls are then needed to establish confidence.

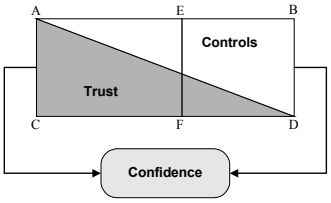

Figure 3. The Relationship between Trust, Controls and Confidence [18]

The Risk Appetite Line (E-F) is dependent on the levels of trust between two individuals. If there is a high degree of trust evident, the focus of the line will be more on the trust area and less on the control area. If there is a low degree of trust between the two parties, the focus will be more on controls and less on trust, resulting in the line being directed closer to the right. It is desirable that a balance is reached; it would be rare to have complete trust and no controls, or the opposite, complete controls and no trust.

TABLE I. TRUST AND CONTROL DIAGRAM NARRATIVE

Position	Description
Triangle ABD	• This is the control area (protected by controls)
Triangle ADC	• This is the trust area (protected by trust)
Line EF	• The risk appetite (i.e. the desire or willingness to take on various levels of risk)
Rectangle ABDC	• This is the business process or transaction area

While the relationship described refers to organizational confidence, the concept of how trust and controls influence confidence can be easily applied to the OSN context. The interacting individuals are replaced by the online user and the combination of social networking service provider and application. Each user has their own Risk Appetite line, which reflects their level of trust offered, based on the controls present in the environment. This results in an increased level of confidence and trust for the user.

In order to reduce uncertainty and increase trust, the introduction of an effective system of controls can overcome this challenge. Systems of controls become applicable in an OSN environment for several reasons. As controls are a planned measure or countermeasure designed to mitigate a risk, their primary application is that of protecting users and their information from individuals desiring to harm them [20]. These controls are often combinations of people, processes and

tools put in place to prevent, detect or correct issues caused by unwanted events. Their desired outcome is to create a carefully designed control framework that weaves the various types of controls together and protects the organization from risks [16]. These controls are categorized according to the function they perform, with the main functional categories being Preventative, Detective and Corrective as seen in figure 4 [20].

A comprehensive set of controls must be designed around these core functional categories in order to be effective and reduce the level of uncertainty existing between individuals. Not only is the level of trust between individuals important, but so too is the relationship between users and the system.

Preventative	• This category of controls is aimed at avoiding any unwanted situations
Detective	• This category of controls is aimed at countering the error factor • Alert when unwanted event has occurred, but always after event has taken place
Corrective	• This category of controls is aimed at restoring the system to its accepted state

Figure 4. Summary of Three Control Theory Perspectives (own compilation)

Controls implemented within these social networking applications can limit uncertainty and help develop confidence and trust in the system. The following section will discuss the other element needed to enhance the relationship between users and the system, namely the IDM practices and processes.

IV. IDENTITY MANAGEMENT WITHIN ONLINE SOCIAL NETWORKS

IDM is defined as the management of identification, authentication and authorization information, as well as the use of this information to authenticate and properly authorize principals in a computer network or distributed system, such as the Internet [21].

The common attribute of IDM practices within the current online environment is the "one to many" relationship between user and service provider. These IDM practices aim to manage one user across many service providers. However, the more challenging aspect of IDM is the implementation of the process within these service providers. Users are able to create multiple user profiles or accounts that can be accessed within one online service. Systems and processes need to be implemented that can manage these users and achieve a satisfactory level of user-to-profile linking. Current IDM practices will now be briefly discussed. These practices include the core concepts of Single Sign-On (SSO) and Identity Management Systems (IMS). Current Identity Management Models (IMD) will now be discussed.

A. Current IDM Practices

Presently, formal IDM is a practice exhibited at corporate level, with many large software vendors providing IDM solutions. These solutions are primarily focused on managing employees across internal boundaries. The core concepts of these IDM solutions are:

1) Single Sign-on

Single sign-on is the ability of a user to create a single set of login details, which they can share and gain access to numerous systems or networks. Efficiency gains are experienced, with users no longer re-prompted for login details across applications and services. This is only possible if the service provider is partnered to the SSO provider [6].

2) Identity Management Sytems (IMS)

An IMS refers to an information system or to a set of technologies that can be used to support the management of identities [22]. IMS align to three main categorizations, as shown in figure 5.

It is apparent from the categorization provided [22], that social networking IMS are typically of type 1. Social network providers such as Facebook and MySpace administer the creation and management of all profile creation and changes, as well as the authentication and authorization of these profiles during everyday use of the service. For these very reasons, they exhibit the key characteristics of type 1 IMS.

IMS Type	Description
Type 1 Core IMS	• Account Management • Authentication • Authorization Practices
Type 2 Additional Function + IMS	• Analysis of User Data; • Data Warehousing
Type 3 IMS Independent	• User/Client Orientated; • User Privacy

Figure 5. IMS Classification Summary (own compilation)

The comparison in figure 4 shows the attributes of the three IMS types. Based on the comprehensiveness of type 1 IMS, this reiterates the use of these systems within online social networking services. Providers have developed a highly intricate network of relationships between users worldwide. Such services require most of the tabled attributes in order to perform effectively, from both user and provider's perspective.

	Identity Management System Classification		
Identity Management System Characteristics	Type 1	Type 2	Type 3
Applications	✓	x	x
Data Warehousing	✓	✓	✓
Centralized User Management	✓	✓	✓
Profile Monitoring	✓	✓	✓
Scalable	✓	x	x
User Control	✓	x	x
User Privacy	x	x	x

Figure 6. Identity Management Systems Summary (own compilation)

B. Identity Management Models (IDMM)

The IDMM to be discussed are the most commonly exhibited models identified within organizations and service providers worldwide. At the conclusion of this section, the various models will be compared and discussed.

Currently, the Isolated User Identity Model (ISUIM) is the most common IDM model used. Service providers act as both credential provider and identifier provider to their users. They control the service domain and allocate identifiers to users. This model requires that each user possess an identifier for access to each isolated service [23]. This model is attractive for service providers, due to its ease of management. This is

characterized by the simple process whereby a single user gets assigned a single set of login credentials. However, as demands increase throughout the online environment, users are being overloaded with identifiers and credentials that they need to remember and manage. The management of these multiple credential sets almost becomes an impossible task [24].

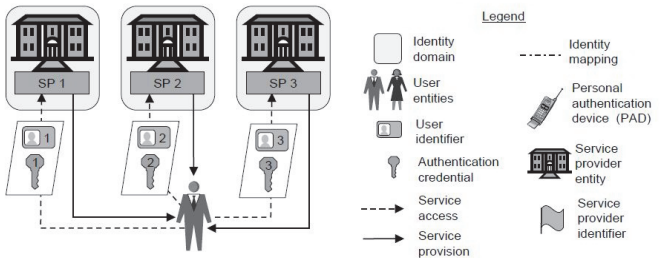

Figure 7. Isolated User Identity Model (ISUIM) [23]

The Federated User Identity Model (FUIM) attempts to address inefficiencies found within ISUIM. Identity federation is a set of agreements, standards and technologies that enable a group of service providers to recognise user identifiers from other service providers within a federated domain.

In federated identity domains, agreements are established between SPs so that identities from different SP domains are recognised across all domains. This incorporates a mapping process to be performed by each service provider, which stores the user and credential combinations for later evaluation [23].

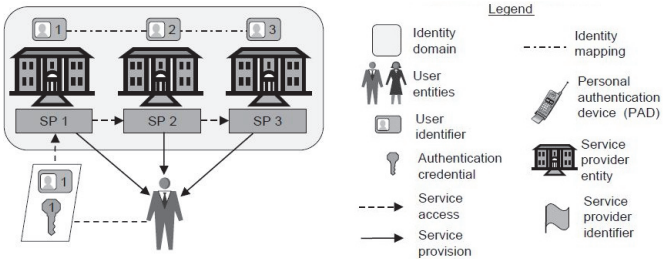

Figure 8. Federated User Identity Model (FUIM) [23]

The Common User Identity Model (CUIM) is relatively simple in operation. Here, a single authority or entity acts as the exclusive user credentials provider for all service providers. A user can then access all service providers by using the same set of credentials.

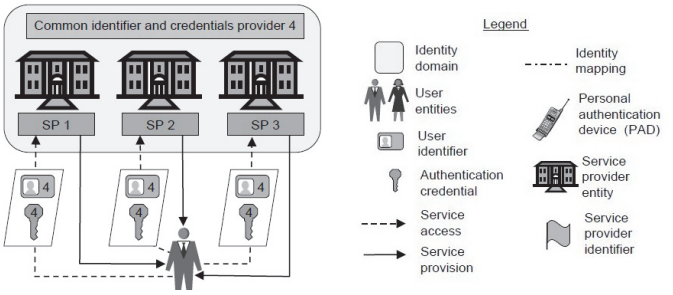

Figure 9. Common User Identity Model (CUIM) [23]

The *Single Sign-On Identity Model* (SSOIM) allows the user to be authenticated by one service provider and in turn, to be considered authenticated across several other service providers as well, by using the same set of credentials. Typically, there is only one identifier and credential provider which is responsible for the generation of these credentials, as well as the authentication when interacting with the user [25].

This model is very similar to the FUIM, where the user can access all service providers with the use of a single set of credentials. The difference arises in the mapping process needed for the federated model to be effective. Instead of each service provider still maintaining their own unique credentials per user, the same credentials set will now be accepted by any other provider.

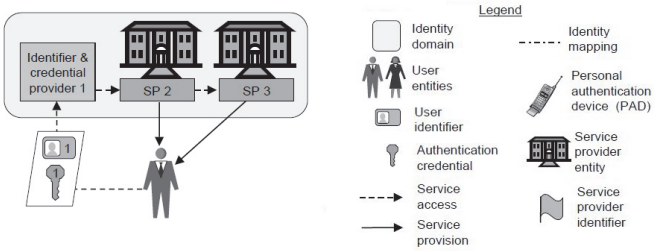

Figure 10. Single Sign-On Identity Model (SSOIM) [23]

Figure 11 below depicts the comparison between the four main identity management models evident throughout organizations and service providers worldwide. All four models are characterized by the same service provider role of credentials and identifiers provider. However, only the isolated and federated models have locally generated user credentials. What this means is that service providers have control over the service domain and the allocation of identifiers to users. Common and single sign-on have their user credentials generated by an independent third party. The isolated model is primarily used for a single domain environment, where users will operate within the service provider's domain exclusively. This can prove problematic for the user, as the management of multiple username-password credential sets is a tedious task.

		Service Provider Role		Service Provider Type		Domains Accessible	
User Identity Model Type	Acronym	Credential	Identifier	Independent	Local	Single	Multiple
Isolated	ISUIM	✓	✓	✘	✓	✓	✘
Federated	FUIM	✓	✓	✘	✓	✘	✓
Common	CUIM	✓	✓	✓	✘	✘	✓
Single Sign-On	SSOIM	✓	✓	✓	✘	✘	✓

Figure 11. Identity Management Model Summary (own compilation)

OSN are domains where anonymity is easily created and ensured. The information needed to create a new profile is general and non descriptive [26]. The models mentioned are all effective in their designated environments, but fall short of encapsulating the world of social networking.

C. *Current IDM evidence within Online Social Networks*

In mid 2008, Facebook developers announced a new service to their growing platform that was an attempt at a complete IDM solution for all Facebook users. This was entitled Facebook Connect, and was officially launched in December 2008 [27]. Some key features are (1) *Trusted Authentication*, which enables users to connect their Facebook account with any partner website using a trusted authentication

method and (2) *Real Identity,* which enables users to represent themselves with their real names and identities as used in Facebook while Internet browsing.

The IDM link achieved by Facebook Connect is that of an SSO identity model wherein Facebook users may use their original Facebook login credentials to access the partner websites affiliated with the Connect service. In response, MySpace announced a very similar service in 2008 entitled MySpace Data Availability. This additional service displayed similar characteristics to Facebook Connect, including enabling users to have their MySpace profiles follow them around as they conduct their Internet browsing [28].

As mentioned earlier, these forms of IDMM are effective for environments where the identity is verified or where there is no real threat should the user not be who they claim to be. However, within the OSN context, the application of this SSO model attracts the same shortfalls when required to effectively manage identities. Facebook Connect and MySpace Data Availability are unable to accurately authenticate the user's profile and are only providing a further service that extracts user Internet activity. The underlying IDM problems of user anonymity and the ability to create multiple profiles still exists.

V. EVALUATING CURRENT CONTROLS

In order to test the various controls and processes presented by these OSN service providers to their users, a detailed experiment was designed and conducted for analysis. Each area was identified due to the contribution to the problem area, and was assessed for possible vulnerabilities.

A. Profile Creation and Interactions

The core feature behind the design of the experiment was creating a number of fictitious user profiles, each with a specific character focus and created by the researcher. These were duplicated across both MySpace and Facebook service providers. These profiles were used to conduct the daily activities of the average social networking user. Each profile had an associated character type linked to it, and this was the style and attitude of interaction used during the experiment.

TABLE II. SUMMARY OF EXPERIMENT ASSESSMENT AREAS

Assessment Area	Assessment Items
Age Controls	• **Age Verification during profile creation** • **Ability to search users by age** • **Ability to send underage users friend requests** • **Ability for underage users to interact with adults** • **Search groups where teen activity would be high**
Privacy Controls	• **Default setting when creating a profile** • **Ease of use – changing of privacy settings** • **Public versus Private profile settings**
Profile Controls	• **Management of friends** • **Blocking/Reporting of unwanted users**
Identity Management – Service Provider	• **Multiple profiles created by single user** • **Multiple profiles share same password** • **Identity Management** • **All created profiles linked to a blocked user**
Administrator Effectiveness	• **Treatment of reported/blocked users** • **Feedback from reporting/blocking requests**

B. Key Assessment Areas

All areas are closely linked to user trust of the system and fellow users, as well as any IDM practices currently being employed in an OSN environment. These assessment areas were used to guide the experiment as well as form the primary focus areas of the proposed artefact.

C. Experiment Findings

The key findings from the experiment displayed evidence of shortcomings in several areas of assessment. These findings are as follows, presented per assessment area:

- Age Controls

Through the analysis of the controls presented by both service providers, it is apparent that several controls exist and are effective, but the controls relating directly to the individual identities and the management thereof are lacking and highly ineffective. Both service providers have a minimum age for users to create a profile. This minimum age control was evaluated and found to restrict any underage users from creating a profile, but when tried later with a different year of birth, the profiles were created.

Similarly, age controls were not present in areas where teen and underage activity was common, allowing users of any age to interact and communicate with these users.

- Privacy Controls

Both service providers presented adequate controls to establish user trust through their ability to protect user privacy and manage profile privacy settings.

- Profile Controls

Both service providers presented effective controls for the management of friends, which include the friend invite functionality of searching and sending friend requests.

The contrasts arose when investigating the reporting and blocking controls of unwanted contacts. This functionality should be the most effective as this is the only means through which a user can remove any unwanted contacts from their social networking environment. Facebook exhibited the most effective controls in this area; however the reporting of users proved to be questionable.

It is evident that these service providers have no IDM processes within this area to ensure that users are always protected from unwanted contact. Blocking controls must ensure no further contact is ever possible from that blocked individual, even if attempts are made to create new profiles to continue harassment. User trust in the system and the service providers will suffer if they feel they are not in control of their interactions and that the service providers do not place their safety in high regard.

- Identity Management – Service Provider

It is evident from the experiment in this area that there are no forms of IDM processes existing within the OSN environment. This conclusion excludes the formal profile creation process which is a form of IDM in its simplest application. Findings in this area present a situation where service providers have no ability to manage multiple

profiles by single individuals. This is further evident when blocking unwanted users. Profiles created by blocked users remain active and able to contact complainants.

Based on these findings, it can be concluded that effective IDM controls and processes are lacking in the OSN environment. This directly affects user trust levels in the system, as blocked users may still make contact through other fake user profiles after the blocking has taken effect.

- Administrator Effectiveness

During the experiment, the effectiveness of service providers' administrators was assessed when handling blocking and reporting of users. This included the treatment of these users and also the feedback provided to users after performing one of these actions.

It was evident that both service providers were effective in the blocking of users and immediately removed them from the complainant's friend list. However, as discussed earlier, the final result when assessing the effectiveness of administrators when blocking users was ineffective. This was due to the ability of these blocked users to create a new profile and perform the same harassing interactions.

VI. SOCIAL NETWORKING CONTROL SET

Based on the findings gathered during the experiment, it was evident that several areas presented concerns for users These concerns were as a result of no apparent controls present to prevent and discourage certain behaviour from users. It was also evident that where various controls were in place, the level of effectiveness was questionable. The artefact presented is in the form of a set of recommended controls to be implemented by social networking providers to ensure effective IDM as a means to enhance user trust. The artefact will comprise of newly proposed controls, as well as any existing controls proving effective in their current application. Table III shows a summary of the Social Networking Control Set.

The purpose of this set of controls is to increase the trust levels of users through the implementation of effective controls. It was established that if there are low levels of trust experienced, the implementation of controls will increase the level of user confidence, resulting in a higher degree of trust displayed. Although no operational results are evident from the proposed artefact, implementation and the study thereof will form the basis of future research in this area.

TABLE III. SUMMARY OF SOCIAL NETWORKING CONTROL SET

Control Group	Control Name	Control Description	Control Type
Age Controls	• Email registration	• Service providers must log all email addresses that fail the initial age verification control at profile creation. • To ensure effectiveness, email address and username and surname must be logged to prevent the same user with a new email address variation from registering.	Preventative
	• Underage Communication	• If contact is attempted between an adult user and an underage user, the adult must input the younger user's email address as confirmation.	Preventative
	• Underage User Privacy	• All underage users must be protected by the service providers' administrators by default, and cannot make changes to privacy settings.	Preventative
	• Group Age	• Service providers and group creators must apply recommended age restrictions to these various groups. • No adults should be able to search or find groups relating to teen interests and likes.	Preventative Detective
	• User Search Age	• Service providers must either remove ability to search for users by age completely or make the youngest search age 18 year olds.	Preventative
Privacy Controls	• Profile Privacy Settings	• Service providers must exhibit strong controls that protect the users' privacy and ensure users are protected by default.	Preventative
Profile Controls	• Friend Request	• Service providers must ensure that the controls in place to manage user profiles are effective and easy to use. • Adult users should not be able to send friend requests to underage users without email address as confirmation.	Preventative
	• Messaging	• Messaging controls must be in place to ensure that only friends can send and receive messages between each other.	Preventative
	• User reporting and Blocking	• When a user requests to report another user, this must be enforced immediately. • Blocked users must not find complainant's profile through a user search. • It is proposed that the blocked user's name and profile details be flagged so that they cannot simply create a new profile with similar details.	Corrective
Identity Management Controls	• User Verification	• Effective user verification process to be part of registration process. Must include submission of government issued identification document or similar. • Documents to be submitted for profile activation; else a status must appear on profile as "unconfirmed". This acts as a warning that the identity of the profile is unconfirmed.	Preventative
	• Profile Linking	• Service providers are encouraged to create automated processes that filter created profiles for various triggers. • These filters act as triggers for investigation. Investigations could request identity verification or similar means to confirm the individual and remove profile alerts.	Detective Corrective

VII. CONCLUSION

In conclusion, it is evident that online social networking has several areas where controls and effective IDM processes are needed. These vulnerabilities are open to exploitation by malicious users, in turn reducing the levels of trust exhibited by users in the system and in other users.

In order to address these shortfalls and increase trust levels, an experiment took place to assess the current controls and identity management processes evident within the current social netwroking environment. Based on the experiment findings, a proposed set of controls was presented which aimed to provide an effective means to enhance user trust through their implementation and management. User trust and confidence for both the system and other users are market requirements, and the implementation of an effective set of controls can assist in achieving them.

REFERENCES

[1] Benevenuto, F., Rodrigues, T., Cha, M. and Almeida, V. (2009). *Characterizing User Behaviour in Online Social Networks*. Computer

[2] Science Department, Federal University of Minas Gerais, Brazil. Retrieved 4 May, 2010, from http://portal.acm.org

[3] Alexa Facebook (2010). Web Information Company. Web Usage Report. Retrieved 4 May, 2010, from http://www.alexa.com

[4] Alexa MySpace (2010). Web Information Company. Web Usage Report. Retrieved 4 May, 2010, from http://www.alexa.com

[5] Fidis WP 2. (2006). D2.6: Identity in a Networked World – Use Cases and Scenarios. Future of Identity in the Information Society. Retrieved 5 August, 2008, from http://www.fidis.net

[6] Jones, H. and Soltren, J. (2005). Facebook: Threats to Privacy. *Electrical Engineering and Computer Science*. Vol. 6, pp. 30-106.

[7] Online Social Networking (2010). *How online social networks work*. Retrieved on 10 May, 2010, from http://communication.howstuff

works.com

[8] Hinduja, S. and Patchin, J. (2008). Personal information of adolescents on the Internet: A quantitative content analysis of MySpace. *Journal of Adolescence.* Vol. 31, pp. 125–146.

[9] Hansen, M., Pfitzmann, A. and Steinbrecher, S. (2008). Identity Management throughout one's whole life. *Information Security Technical Report* (2008).

[10] Computer Fraud (2008). Woman accused of bullying teen on MySpace. *Computer Fraud and Security*. June 2008, pp. 1-2.

[11] Social Network Concerns (2010). Facebook vs MySpace: Concerns on Social Networking. Retrieved on 17 May, 2010, from http://theambitious.org

[12] Social Media Concerns (2010). *Social Media Risks: The Basics*. Retrieved on 11 May, 2010, from http://www.csoonline.com

[13] Beldad, B., de Jong, M. and Steehouder, M. (2010). How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust. *Computers in Human Behaviour.* Vol. 26, pp 857–869.

[14] Shin, D. (2010). The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption. *Interacting with Computers.* Vol. 22, No. 5, pp. 428-438.

[15] Dwyer, C., Hiltz, S. and Passerini, K. (2007). Trust and privacy concern within social networking sites: a comparison of Facebook and MySpace. *Proceedings of the Thirteenth Americas Conference on Information Systems (2007).*

[16] Ten Kate, S. (2009). Trustworthiness within Social Networking Sites: A study on the intersection of HCI and Sociology.

[17] Antheunis, M., Valkenburg, P. and Peter, J. (2009). Getting acquainted through social network sites: Testing a model of online uncertainty reduction and social attraction. *Computers in Human Behaviour.* Vol. 26, pp. 100-109.

[18] Mayer, R., Schoorman, D. and Davis, J. (2007). An integrative model of organizational trust: past, present, and future. *Academy of Management Review.* Vol. 32, No. 2, pp. 344-354.

[19] Neuliep, J. and Grohskopf, E. (2000). Uncertainty reduction and communication satisfaction during initial interaction: An initial test and replication of a new axiom. *Communication Reports.* Vol. 13, No. 2, pp. 67-77.

[20] Flowerday, S., and von Solms, R. (2006). Trust: an Element of Information Security. Presented at IFIP/SEC 2006, Karlstad, Sweden. Published in S. Fischer-Hubner, K. Rannenberg, L. Yngstrom, S. Lindskog (Eds.). Security and Privacy in Dynamic Environments. 87-98. IFIP. USA: Springer.

[21] Berger, C. and Calabrese, R. (1975). Some explorations in initial interaction and beyond: Toward a developmental theory of interpersonal communication. *Human Communication Research.* Vol. 1, pp. 99-112.

[22] Giblin, C. and Hada, S. (2008). Towards separation of duties for services. IBM Zurich. Retrieved on 25 August, 2010, from http://www.zurich.ibm.com

[23] Oppliger, R. (2004). Microsoft .NET Passport and identity management. *Information Security Technical Report*. Vol. 9, No. 1, pp. 26-34.

[24] Fidis WP 3. (2005). D3.1: Structured Overview on Prototypes and Concepts of Identity Management Systems. Future of Identity in the Information Society. Retrieved on 5 August, 2008, from http://www.fidis.net

[25] Josung, A. and Pope, S. (2005). User Centric Identity Management. CRC for Enterprise Distributed Systems Technology (DSTC Pty Ltd). Retrieved on 10 April, 2008, from http://sky.fit.qut.edu.au/josang/papers

[26] HKSKR (2008). Identity Management. Hong Kong Special Administrative

[27] Zhoa, S., Grasmuck, S. and Martin, J. (2008). Identity construction on Facebook: Digital empowerment in anchored relationships. *Computers in Human Behavior*. Vol. 24, pp. 816–1836.

[28] Facebook Connect (2009). Facebook Developers Blog. [On-line]

Available: http://developers.facebook.com [Accessed: 23 October 2010]

[29] MySpace Data Availability (2009). MySpace Developers Forum. Retrieved on 23 October, 2010, from http://developer.myspace.com

[30] Hobson, D. (2008). Social Networking – Not always friendly. *Computer Fraud and Security*. Feb 2008. pp. 4-6.

[31] Internet Security (2007). Keeping children safe online. *Biometric Technology Today*, June 2007. pp. 4-5.